Locating Central Actors in Co-offending Networks

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

Vahid Dabbaghian
MoCSSy Program, The IRMACS Centre
Simon Fraser University
British Columbia
Canada
Email: vdabbagh@sfu.ca

***Abstract*—A co-offending network is a network of offenders who have committed crimes together. Recently different researches have shown that there is a fairly strong concept of network among offenders. Analyzing these networks can help law enforcement agencies in designing more effective strategies for crime prevention and reduction. One of the important tasks in co-offending network analysis is central actors identification. In this paper, firstly we introduce a data model, called unified crime data model to bridge the conceptual gap between abstract crime data level and co-offending network mining level. Using this data model, we extract the co-offending network of five years real-world crime data. Then we apply different variations of centrality methods on the extracted network and discuss how key player identification and removal can help law enforcement agencies in policy making for crime reduction.**

I. Introduction

Computational Criminology is an emerging interdisciplinary research field promoting the use of computational methods and mathematical models in advanced studies of social phenomena related to crime and other forms of illegal activities such as terrorism. Research in computational criminology shows promising results [1], [2], [3] that underscore the enormous potential for serving practical needs in crime analysis and prevention, namely as instruments in crime investigations, as an experimental platform for supporting evidence-based policy making, and in experimental studies to analyze and validate theories of crime [4], [5]. The work presented here explores properties of criminal networks in large data sets and as been inspired by practical experience with mathematical modeling and computational analysis techniques in the study of crime events, spanning a wide range of criminal activities, including opportunistic and violent serial crimes [6], [4], [7].

This paper addresses the problem of locating *central actors* in co-offending networks. Identifying the key actors of a network is a common problem studied in social networks. Central actors are potentially more important and also have a higher influence on other actors [8]. Recognition and removal of these nodes from the network is an aspect of fundamental importance in the study of crime, especially organized crime, for splitting a network and for making it dysfunctional [9]. Despite the importance of this problem for law enforcement agencies, to the best of our knowledge, there is no widespread research on centrality analysis in large scale co-offending networks to show if and how this kind of analysis can help in crime reduction and prevention or other efforts aiming at destabilizing the co-offending network structure. The lack of research in this field can be explained with the sensitivity of crime data, not permitting public real-world crime data sets.

Based on a research memorandum of understanding between ICURS[1] and "E" Division of Royal Canadian Mounted Police (RCMP) and the Ministry of Public Safety and Solicitor General, five years of real-world crime 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 (cf. Section V). The data set is based on arrest-data.

The research presented here uses five important centrality measures and compares different experiments on the extracted co-offending networks. Specifically, we try to answer two questions: First, what is the effect of central actors removal on the crime rate reduction and how does this change the co-offending network structure; second, how does centrality analysis and central actors elimination work in the dynamic and time-varying co-offending network. These two questions are answered in detail in Section V.

Besides mining and analyzing crime data sets to identify potentially useful patterns, another main step is modeling the data. We propose here a comprehensive crime data model, called *unified crime data model*, and use this model as the basis for our co-offending network extraction and analysis. We contend that central aspects considered in the work discussed here carry over to a wide range of large data sets studied in intelligence and security informatics to better serve law enforcement and intelligence agencies.

The paper is organized as follows. Section II discusses related work. Section III defines the unified crime data model and explains how the co-offending network model is derived. Concepts of centrality and their meaning in co-offending networks are presented in Section IV. Next, Section V gives a general characterization of the crime data set and also presents and discusses the experimental results, and Section VI concludes the paper.

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

II. Related Works

With academic and societal awareness of the importance of social networks increasing, law enforcement 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 [13]. Groups and organizations operating within this network to engage in conspiracies, terrorist activities and crimes like drug trafficking typically operate in a concealed fashion, trying to hide their illegal activities, but 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 resources readily available to investigators, such as police arrest data and court data, and study them using social network analysis methods. In turn, social network analysis can provide useful information about individuals as well. For example, investigators could determine key players, and make subject them to closer inspection. In general, 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. Reiss [13] concludes that the majority of co-offending groups are unstable, and their relationships are short-lived. This is corroborated by McGloin et al., [15] 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. [14] also found that co-offenders have many different partners, and are unlikely to commit crimes with the same individuals over time. However, Reiss [13] 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 were obtained on very small datasets: 205 individuals in [14], and 5600 individuals in [15], and may therefore not be representative.

These studies just analyzed co-offending networks. Smith [18] 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., [19] 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 network is important, because vehicles provides new investigative points.

A slightly different take on widening the scope of crime network analysis was taken by Xu et al. [17], 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 [16] 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. [10] 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 [17] 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.

The success of integrating crime network analysis with police workflow depends crucially on its ability to reduce crime level. With regard to this, Liu et al. [21] proposed a game-theoretic framework for key player identification. They defined key players as the offenders who, once eliminated, generate the highest possible reduction in aggregate crime level. The authors showed that key players are not necessarily the most active criminals in a network.

Identification of key players in a social network is a well-established research problem in the form of node centrality analysis, the measurement the structural importance of actors in an entire network [27], or within a group. As Liu showed, detecting key players is an important task in co-offending network analysis, the results of which may help law enforcement agencies design new crime reduction and prevention policies. For instance, in combating the activities of criminal organizations, law enforcement agencies often need to identify the key members of groups of criminals or identify principal vulnerabilities in criminal networks [20].

Based on best of our knowledge, no research has yet given adequate attention to the centrality analysis in large scale co-offending networks. In this work we show how centrality analysis relates to the work of law enforcement agencies, and may help articulate more effective crime reduction and prevention policies.

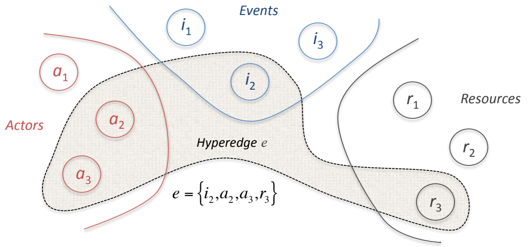


Fig. 1. Hyperedge in the crime data model

III. 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, the formal 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 terms 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, $A = \{a_1, a_2, \ldots, a_q\}$, $I = \{i_1, i_2, \ldots, i_r\}$ and $R = \{r_1, r_2, \ldots, r_s\}$, representing *actors* such as offenders, victims, witnesses, suspects and bystanders; *incidents* referring to crime events of a certain type; and *resources* used in a crime, like mobile phones, tools, vehicles, weapons or bank accounts. A hyperedge e of $\mathcal{E}$ is a non-empty subset of nodes $\{n_1, n_2, \ldots n_p\} \subseteq \mathcal{N}$ 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 refers to a different crime incident. Thus, for any $e, e' \in \mathcal{E}$ with $e \cap I = e' \cap I$, it follows that $e = e'$. Intuitively, a hyperedge e of $\mathcal{H}$ associates a set of one or more actors $\{a_{i_1}, a_{i_2}, \ldots, a_{i_j}\} \subseteq A$ and a set of resources $\{r_{i_1}, r_{i_2}, \ldots, r_{i_l}\} \subseteq R$ with a crime incident $i_k \in I$, that is $e = \{i_k, a_{i_1}, a_{i_2}, \ldots, a_{i_j}, r_{i_1}, r_{i_2}, \ldots, r_{i_l}\}$, as illustrated in Figure 1.

Finally, with each node $n \in \mathcal{N}$ we associate some finite list of attributes $\langle(\alpha_{n,1}, \beta_{n,1}), (\alpha_{n,2}, \beta_{n,2}), \ldots., (\alpha_{n,l}, \beta_{n,l})\rangle$ 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, as well as other specific aspects of crime data sets 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 $\mathcal{E}' = \{\{a, i, r\} | \ \exists e \in \mathcal{E} : \{a, i, r\} \subseteq e, \ a \in A, \ i \in I, \ r \in R\}$. Note that $\mathcal{H}'$ has the same attributes as $\mathcal{H}$. Now, $\mathcal{H}'$ can further be decomposed in a straightforward way into 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. For instance, this is relevant for law enforcement agencies and criminal justice agencies to better understand organized crime and also 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)* ≥ 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

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

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. Also, co-offenders often try to conceal their connections. Hence, one can expect that besides the links based on explicit facts in the crime data additional links can be derived by analyzing 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 2 illustrates an example for deriving a hidden link in terms of 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

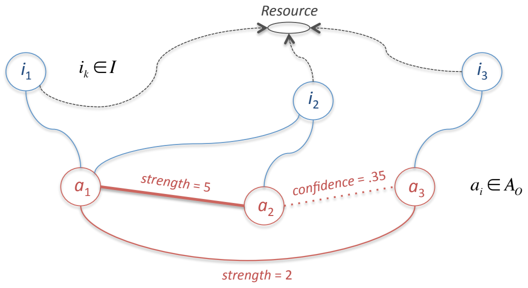


Fig. 2. Criminal activity graph with hidden links

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 on the analysis of explicit links. Note that the concepts of centrality as discussed in Sect. IV need to be extended in order to also include probabilistic links.

IV. Centrality

One of the important problems in studying social networks is identifying the key actors of a network. The importance of actors normally correlates with the centrality of nodes [28], [27]. Central nodes in a social network refer to those nodes that potentially have the highest influence on other nodes [8]. Apparently, recognition and removal of these nodes in/from a co-offending network are of interest from two points of view: splitting the network and its dysfunctionality [9]. This section first reviews important centrality measures and then discusses the application of the centrality analysis to co-offending networks.

A. Centrality Measures

Intuitively, centrality measures identify the actors with the greatest structural importance in a network. These actors often play a central role. The existing centrality measures can be divided into three groups based on how they are calculated: node degree, shortest path and actor ranking methods. Node degree based methods, like indegree and outdegree measures, are local measures that only use the information of the first-level relationship. Methods which use the shortest path length, such as closeness and betweenness, are working based on the shortest path from a node to all other nodes, and therefore are global measures. But the important point is that in these methods centrality of a node is calculated regardless of the position of other nodes in the network. In contrast, actor ranking measures, like eigenvector and PageRank, are also global, but in the process of calculating the centrality of a node the centrality of other nodes is taken into account too.

1) Degree Centrality: Node degree centrality is based on the number of outgoing links of the actors. Each actor that has more links obtain the greater degree centrality value. Therefore, this measure focuses on the most visible actors in the network. An actor with a high degree is in direct relationship or is neighbor to many other actors. Such actors should be recognized by other actors as a main channel of information spreading, indeed, a crucial cog in the network, occupying a central position [22]. In contrast, actors with low degrees are obviously peripheral in the network and these actors are not active in the connection process. Degree centrality of the actor x is [22]:

$$C_D(v) = \frac{d_v}{N-1} \tag{2}$$

where d_v is the number of first level neighbors of v, and N is the total number of actors in the network.

2) Closeness Centrality: The main idea behind the closeness centrality is that actors that can contact quickly other actors in the network, take the central position. The closeness centrality of an actor in a social network is the inverse of the average shortest path distance from the actor to any other actor in the network. This measure shows how much each actor is efficient in spreading information to all other actors. The larger the closeness centrality of an actor, the shorter the average distance from the actor to any other actor, and therefore the better position the actor has in the network to spread information to the other actors. Closeness centrality of the node v is computed as [23]:

$$C_c(v) = \frac{N-1}{\sum_{u \in V} d(u,v)} \tag{3}$$

3) Betweenness Centrality: The betweenness centrality is defined as the number of shortest paths between pairs of nodes that pass through the given node. This centrality measure is based on the idea that an actor is central if it lies between many other actors pairs and it would be traversed by many of the shortest paths connection pairs of actors. The betweenness centrality of the node v is defined as [24]:

$$C_c(v) = \sum_{\substack{u,w \in V \\ u \neq w \neq v}} \frac{\sigma_{uw}(v)}{\sigma_{uw}} \tag{4}$$

where $\sigma_{uw}(v)$ represents the total number of shortest path between each pair of nodes like u and w that pass through node v and σ_{uw} denotes the total number of shortest path from u to w.

4) Eigenvector Centrality: The eigenvector method is an effort to recognize the central actors in terms of the global structure of the network and to pay less attention to local properties. Eigenvector centrality is defined as the principal eigenvector of the adjacency matrix representing the network. The eigenvector of a network is computed using equation [28]:

$$\lambda v = Av \tag{5}$$

where A is adjacency matrix of the network, λ is a constant (eigenvalue), and v is the eigentvector. The idea behind this approach is that actors are central if they have central neighbors. So centrality of an actor does not only depends on the number of its neighbors, but also on their centrality in the network.

5) PageRank Centrality: PageRank method [25] is a variant of the Eigenvector centrality measure which basically is used for ranking the web pages. PageRank models the behavior of a surfer of the web pages and tries to propose a ranking of web pages based on his behavior. The surfer starts at a random page and move from per page to another page using the outgoing links. For jumping from a page to another one, the outgoing links are selected uniformly at random. Also the surfer with a probability can jump to any other page.After many iteration a probability for hitting each page is calculated which shows its chance of being visited by the surfer. This method also can be applied on social networks to rank actors. PageRank of the node u is computed as:

$$C_p(u) = \frac{1-d}{N} + d(\sum_{\forall v: v \rightarrow u} \frac{C_p(v)}{N(v)}) \tag{6}$$

where N is the number of nodes in the network, N_v is the set of all nodes connecting to v and d is the probability of continuing the process of moving on the network and not jumping to a random page which is generally set around 0.85.

B. Centrality in Co-offending Networks

Key players of co-offending networks are not essentially the most active offenders. Offenders removal from the co-offending network has direct and also indirect effects. As a direct effect, fewer offenders contribute to the aggregate crime level. The indirect effect is the modification of the network topology. Then this network structure modification can change the criminal efforts of the remaining offenders and may reduce the level of happening crimes.

Structure of the networks is the key factor in the measure of affect of central players elimination. In the covert crimes network such as terrorist networks, key players elimination is not counted as an efficient network destabilization tactic. Since these networks structure are not like typical hierarchical organizations. Indeed, key feature of these networks is that they are cellular and distributed [26]. But clearly, destabilizing a hierarchical network would be relatively easy compared to a distributed decentralized one.

Now, let's look at the centrality analysis of a real co-offending network. Figure 3 shows the second largest component of the extracted co-offending network. Table I lists the ranks of the key nodes A to L according to the chosen centrality measure. The numbers within the table indicate the ordering of the Top 5 offenders identified by each measure. For example, offender E was identified as the second most important offender by eigenvector centrality, but only 4th with betweenness centrality.

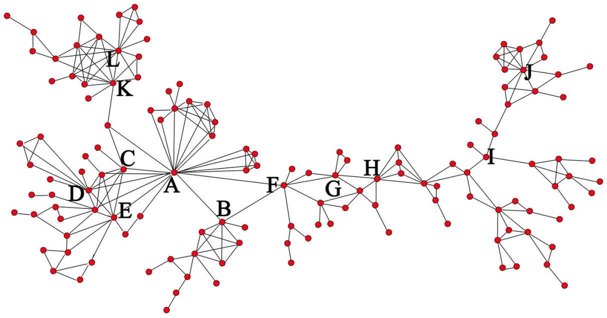


Fig. 3. Visualization of the second largest component

Measure	**Offenders**										
	A	B	C	D	E	F	G	H	J	K	L
Degree	1			3					4	5	2
Betweenness	1	3		5	4	2					
Closeness	2	4				1	3	5			
Eigenvector	1		5	3	2				4		

TABLE I
CENTRALITY MEASURES ON THE SECOND LARGEST COMPONENT

Although all the different centrality measures tended to identify different individuals in varying order, all but one measure agreed that offender A was most important. This strong result was somewhat surprising given that in total 11 offenders were identified to be in the Top 5 by different measures. Offender A does seem to be an important offender in the network, as this offender has the largest number of edges, is involved in 3 cliques of at least size 5, and would fragment the network into 4 pieces if removed. Without this information, a police force could capture multiple offenders, not realizing that specifically targeting only offender A in the network would have a huge impact on the network and remove by far the most important offender. It is also interesting to see that the above 4 measures identified quite a few offenders along the shortest path between the two furthest nodes. This path travels through offenders K, C, A, F, G, H and J.

In the section V, the results of applying these centrality methods on the complete co-offending network and different comparison experiments outputs are discussed.

V. Evaluation Experiments

We believe network centrality analysis can help law enforcement agencies develop strategies for crime reduction and prevention. The current strategy is trivial, from a network perspective: remove those offenders that are most active (nodes with high degree) or commit the most severe crimes. Reiss's argument some offenders actively recruit new offenders, [13] combined with Liu et al.'s finding that key players (assumed to be the recruiters) are not necessarily the most active criminals in a network [21] warrants a close look at key player identification in co-offending networks. The hiddenness of links and the time-varying structure of these networks necessitate thorough analysis and experimentation to extract the facts to base law enforcement policy on.

Several experiments were conducted to evaluate the appropriateness of various centrality measures (degree, closeness, betweenness, eigenvector and PageRank) for identifying important actors in co-offending networks. Ideally, one would test the hypothesis that removal of central actors reduces crime rate. The data required for testing this hypothesis is currently not yet available, and reconstructing the crime rate from the co-offending network (clique finding) is computationally prohibitive. It is, however, possible to investigate the effects of removal of central nodes on the network structure.

The crime rate and network structure are intricately linked. In particular if $n_{u,v}$ is taken as the multiplicity of edges between offenders u and v, the degree of an actor is equal to the number of crimes this offender committed. The overall crime rate, however, is not equal to the total number of links in the network, since every event involving k offenders translates to a complete graph of size k in our co-offending network. Thus, characteristics of network structure may give some intuition about our original question, a connection which we will revisit in discussing our first experiment.

We also investigate the effects of removing central nodes selected using the static network (all two, three, or four years worth of data combined) and those selected using a dynamic network (one network for each year). The thought is to account for possible (lack of) persistence in the co-offending network, possibly putting more emphasis on more recent crimes in determining if a person is likely to commit new crimes. Priority given to more recent crimes reflect a real-world bias/predilection/skew of assigning more importance to more recent crimes in determining the criminality of an offender. A small difference between the selections from the static and dynamic networks would lend credibility to the hypothesis that important offenders do not change their game. A larger difference would mean the co-offending network is to some extent transient: offenders cease activity, and other, new offenders start.

All figures below are of offender removal experiments: the top 1%, 5%, 10% and 20% of nodes according to each centrality measure is removed from the network, and a line plot of a statistic on the resulting network is shown. A thick dotted line indicates the reference level of the statistic, being either the expected value of the statistic given the number of offender that are removed, or the value of the statistic over the whole network if its change due to node removal cannot be forecast.

A. Data Set

The below experiments were conducted on a data set made available by the "E" Division of the Royal Canadian Mounted Police (RCMP), as a result of a research memorandum of understanding between ICURS, the RCMP and the Ministry of Public Safety and the Solicitor General. The data contains five years (2001-2006) of real-world crime 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. PIRS contains information about all reported crime events (≈4.4 million) and all persons associated with a crime (≈9 million), from complainant to charged. In addition, PIRS also contains information about vehicles used in crimes (≈1.4 million), and businesses which were involved in crimes (≈1.1 million). Of this dataset, only those offenders that were charged, chargeable, or had a charge recommended, were extracted and used for the following analysis. Being in one of these categories implies that the police were serious enough about the persons involvement in a crime as to warrant calling them 'offenders'. Statistical properties of the co-offending network extracted from these data are listed in Table II.

Metric	Value
# Co-offenders	157274
Average Degree	4
Exponent (λ)	2.29
Average Distance	12.2
Diameter	36
Effective Diameter	16.87
Average Clustering Coefficient	0.39

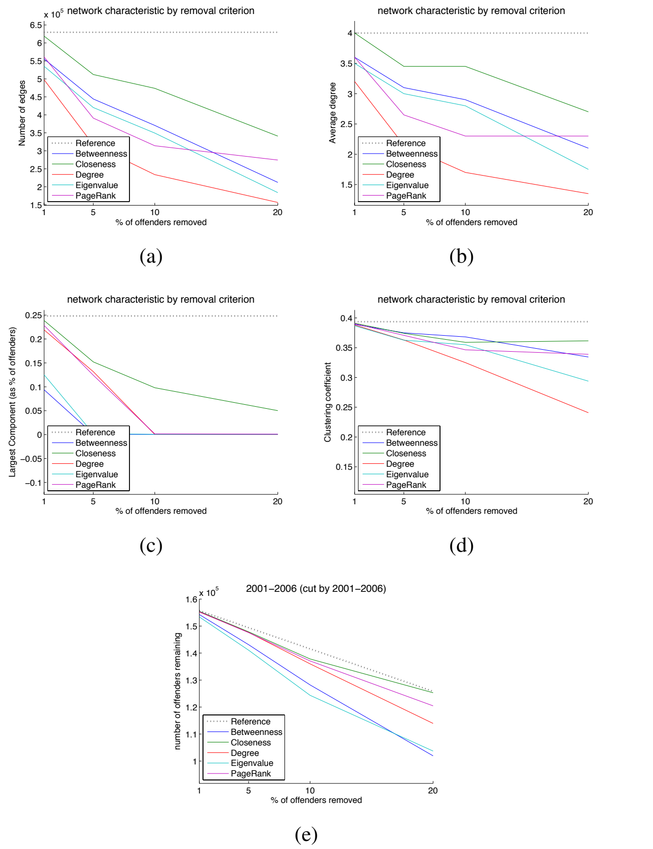
TABLE II
STATISTICAL PROPERTIES OF THE STUDIED NETWORKS

B. Central Nodes Removal Effects

It is common practice that the network in which centrality is measured is the same as the network in which the effects of removal of most central nodes are measured (see 4, provided here for reference). Most of the results are as one should expect: cutting by degree centrality has the largest effect on average degree, cutting by betweenness has the largest effect on the largest component size, exactly what these centrality measures were designed for. One highlight of these figures is the reasonable efficacy of degree centrality-based node removal, the selection method used by law enforcement agencies, for breaking up the network (4(c)), an important feature under our assumption that at least some crime is socially stimulated or facilitated. Other methods (eigenvector and betweenness centrality) can do better, though, partly validating our current research question.

In a crime prevention scenario, and any network that changes over time, this is of course not appropriate: removal happens based on information collected prior to the time of removal, and affects the network after the time of removal. Therefore, we split up the data into 5 networks, one for each year's worth of data, and tested the effects of intervention (central node removal) after the first year, second year, third year and fourth year, identifying central nodes in the network of the previous years and removing those from the network of the following years. For reference, we also include the whole network analysis, in which central nodes were identified in the same (whole) network as they were removed from.

In this experiment, the top offenders according to each centrality measure computed over the network preceding the



(a)

(b)

(c)

(d)

(e)

Fig. 4. Network statistics for the whole network (2001-2006) after removal of the top $x\%$ of offenders, according to different centrality measures.

intervention were removed from the network at the intervention. Since these offenders are assumed to be dominant actors in the network, causing others to offend, other offenders who only commit crimes with (one of) these top offenders are also removed. The effect on the resulting networks after the intervention is illustrated in 5. Only the number of offenders is reported, but the results for other network statistics are quite similar, showing only marginal change.

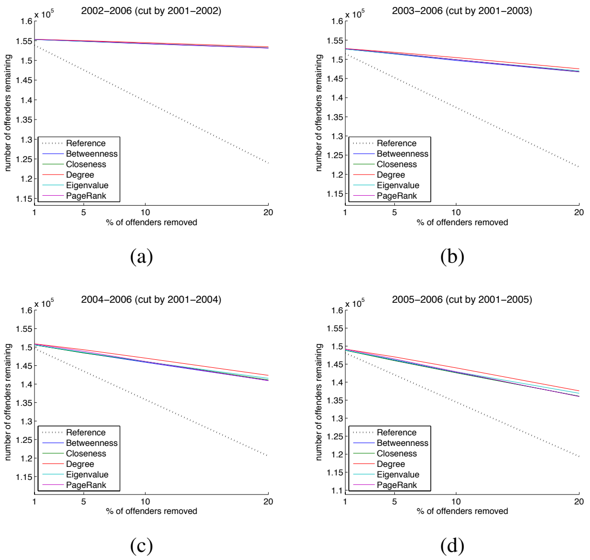
The decrease in the number of offenders in the resulting network is smaller than would be expected (represented by the dashed line). This points to an important feature of the network: transience. III shows the overlap, computed using the Jaccard index

$$J\left(S_1, S_2\right) = \frac{S_1 \cap S_2}{S_1 \cup S_2} \tag{7}$$

between offender sets of subsequent years, and of pre- and post-intervention networks, and it re-affirms the transient nature of the network.

This transience should be interpreted with caution. One could infer that the majority of offenders come into contact with the police only very infrequently, and this is indeed the case. This does not, however, imply that such offenders are incidental criminals; they may have been arrested, and thereby removed from any opportunity to recurr in the data. We currently do not have access to data that would allow us to distinguish between the two, but incidental criminality supposedly being the result of coincidence (as a form of randomness), incidental criminals should be less likely identified as central nodes.

This supposition is supported by III, where the average realised Jaccard index is listed in brackets after J(pre-intervention,post-intervention). The realised Jaccard index is the Jaccard index of the selected set of most important offenders of the pre-intervention network and the set of all offenders in the post-intervention network, divided by its theoretical maximum (when all most important offenders recur in the post-intervention network). III shows that, as the amount of historical information included in the selection of important offenders (the pre-intervention network) increases, the selected most important nodes from the pre-intervention network are more likely to occur in the post-intervention network ($p < 0.01$ for J(2001-2005,2005-2006)). Thus, we have shown that centrality in the co-offending network in the past is at least somewhat informative about criminality in the future, getting back to our original hypothesis.



(a)

(b)

(c)

(d)

Fig. 5. Post-intervention number of offenders for interventions at different points in time.

J(2001–2002,2002–2003)	0.0972	
J(2002–2003,2003–2004)	0.1627	
J(2003–2004,2004–2005)	0.1853	
J(2004–2005,2005–2006)	0.1976	
J(2001–2002,2002–2006)	0.0471	(0.0455)
J(2001–2003,2003–2006)	0.1118	(0.1255)
J(2001–2004,2004–2006)	0.1654	(0.2073)
J(2001–2005,2005–2006)	0.2040	(0.2807)

TABLE III
OVERLAP BETWEEN OFFENDER SETS IN SUBSEQUENT YEARS, AND OVERLAP BETWEEN PRE-INTERVENTION AND POST-INTERVENTION OFFENDER SETS. IN BRACKETS: THE AVERAGE REALISED JACCARD INDEX OF THE SETS OF MOST IMPORTANT OFFENDERS, AS EXPLAINED IN THE TEXT.

	2001-2002	2002-2003	2003-2004	2004-2005	2005-2006
2001-2002	1.0000	0.0972	0.0798	0.0675	0.0569
2002-2003	0.0972	1.0000	0.1627	0.1570	0.1248
2003-2004	0.0798	0.1627	1.0000	0.1853	0.1803
2004-2005	0.0675	0.1570	0.1853	1.0000	0.1976
2005-2006	0.0569	0.1248	0.1803	0.1976	1.0000

TABLE IV
OVERLAP BETWEEN OFFENDER SETS IN DIFFERENT YEARS, MEASURED AS THE JACCARD INDEX.

C. Centrality in Time

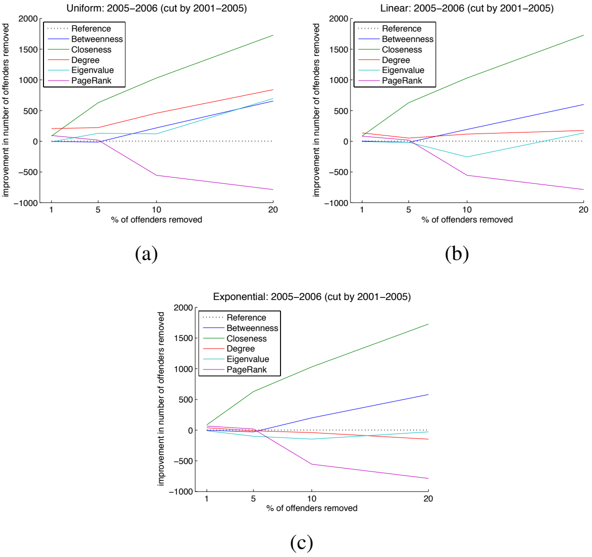
With the five years worth of data batched into individual years, it would seem rather naïve to assign equal importance to events that happened in the first year and events that happened in the last year. This is supported by the overlap between the offender sets of the different years, measured by the Jaccard index in IV. The overlap between two 'time slices' decreases as the amount of time between them increases. This points yet again to the previously mentioned network transience. It also hints at the fact that if we wish to find offenders who will be important after a certain time, we may do well to discount the distant past over the near past.

It may therefore be possible to improve on the previous results by taking into account time, and we compared several time-weighting schemes w:

- none (aggregate network over all years)
- uniform:
$$w_u(C_x, v_i) = \sum_{t=1}^{5} c_x(v_i \in G_t)$$
- linear:
$$w_\ell(C_x, v_i) = \sum_{t=1}^{5} t \cdot c_x(v_i \in G_t)$$
- exponential:
$$w_e(C_x, v_i) = \sum_{t=1}^{5} c_x(v_i \in G_t)^t$$

where $c_x(v_i \in G_t)$ computes centrality x for actor v_i in the network of year t.

If time-weighting changes the set of offenders selected for removal, the structural characteristics of the post-intervention network should also change. The effect on the resulting networks after the intervention is illustrated in 6 as change with respect to the (unweighted) baseline. A positive outcome indicates that the weighting approach was able to further reduce the number of offenders, as compared to the baseline static network. A negative outcome means that the weighting approach actually performed more poorly than without time-weighting. Consistently with the foregoing, only the number of offenders is reported. It is clear that centrality measures measuring more transient features (shortest paths) benefit from taking time into account. Quite counterintuitively, uniform weighting appears to champion the others, suggesting that if historically more important offenders remain important, it does not matter when in history they were important.



(a)

(b)

(c)

Fig. 6. Performance of weighting schemes compared with no weighting scheme (positive values indicate more offenders removed, and hence better performance than unweighted; negative values indicate fewer offenders removed and poorer performance)

VI. CONCLUSION

Centrality analysis is a well-established field of research in social network analysis, and although its applicability in crime prevention is clear, and its potential impact large, it has not gotten the attention it deserves in recent studies of co-offending networks. This is likely due to the limited accessibility of large-scale data sets, leading researchers to focus on either quite theoretical work [21] or limit their analysis to a relatively small sample [20].

In this paper we present results of centrality analysis on a co-offending network extracted from five years of crime data of British Columbia, Canada. The ultimate goal was to select offenders such that an intervention entailing their removal would reduce crime rate. Because explicit crime rate information is not available we analyzed the structure of the resulting post-intervention co-offending networks, particularly the number of offenders consequently (un)available to commit crimes.

Although the efficacy of the investigated centrality measures was limited because of the high transience in the network (offenders ceasing activity and new offenders appearing), we could show that offenders identified as central (by any measure) were more likely to commit further crimes. This effect grew stronger as the amount of information (time observed) used to select central offenders was increased.

Armed with this intuition that time does indeed matter, we compared the performance of centrality measures when computed not over the pre-intervention network as a whole, but over each pre-intervention year individually. We compared several weighting schemes over the centralities per year with unweighted whole-network centrality and found that centrality measures that capitalize on transient characteristics of the network (shortest paths) benefit, whereas centrality measures that rely on more time-stable features of the network did not benefit, or even lost some efficacy. Counterintuitively, equal weighting of all years seemed to be better than discounting the distant past over the near past.

We believe this initial investigation gives rise to many interesting and challenging questions. Future research directions from this could include, in no particular order, an explanation of the reason behind uniform time-weighting coming out on top, analysis of the overlap between the sets of offenders selected by different centrality measures, and exploration of the correspondence between central offenders in different crime type subnetwork.

Acknowledgements

This project was supported in part by NSERC and the CTEF MoCSSy Program at Simon Fraser University. We are also grateful for technical support from the ICURS Institute at Simon Fraser University.

References

[1] 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.

[2] N. Memon, J. D. Farley, D. L. Hicks and T. Rosenorn (eds.), Mathematical Methods in Counterterrorism. Springer, 2009.

[3] P. L. Brantingham, M. Ester, R. Frank, U. Glasser and M. A. Tayebi, Co-offending Network Mining, Springer book on Counterterrorism and Open Source Intelligence, 2011.

[4] 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.

[5] L. Liu and J. Eck (eds.), Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems. IGI Global, 2008.

[6] D. Kim Rossmo, Geographic Profiling. New York: CRC Press, 2000.

[7] 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.

[8] D.M.A. Hussain, D. Ortiz-Arroyo. Locating Key Actors in Social Networks Using. Bayes' Posterior Probability Framework. LNCS 5376, pp. 2738, 2008.

[9] S.P. Borgatti, Identifying Sets of Key Players in a Social Network. Computational and Mathematical Organization Theory. 12(1):2134, 2006.

[10] J.J. Xu, H. Chen, CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery. ACM Transactions on Information Systems, Vol 23 No 2. pp. 201-226, 2005.

[11] R. Adderley and P. Musgrove, Modus operandi modelling of group offending: a data-mining case study. International Journal of Police Science and Management. 5(4): 265-276, 2003.

[12] 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.

[13] A. J. Reiss, Co-offending and criminal careers. Crime and Justice: A Review of Research, 1988.

[14] 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.

[15] J. M. McGloin, C. J. Sullivan, A. R. Piquero, and S. Bacon, Investigating the stability of co-offending and co-offenders among a sample of youthful offenders. Criminology 46 (1), 2008.

[16] 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.

[17] J.J. Xu, and H. Chen, Untangling Criminal Networks: A Case Study. ISI 2003 pp. 232-248, 2003.

[18] M.N. Smith, P.J.H. King, Incrementally Visualising Criminal Networks, iv, pp.76, Sixth International Conference on Information Visualisation (IV'02), 2002.

[19] S. Kaza , and H. Chen, Effect of inventor status on intra organizational innovation evolution. Hawaii International Conference on System Sciences (HICSS-42), Big Island, HI, 2009.

[20] M. K. Sparrow, The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks 13: 251-274. 1991.

[21] X. Liu, E. Patacchini, Y. Zenou and L-F. Lee, Criminal networks: Who is the key player?. CEPR Discussion Paper No. 8185. 2011.

[22] S. Wasserman and K. Faust, Social network analysis: methods and applications. Cambridge University Press, 1994.

[23] G. Sabidussi, The centrality index of a graph. Psychmetrica 31(4), 1966.

[24] P. Carrington, J. Scott and S. Wasserman, Models and methods in Social Network Analysis. Cambridge University Press, Cambridge, 2005.

[25] S. Brin, and L. Page, The Anatomy of a Large-Scale Hypertextual Web Search Engine. Computer Networks and ISDN Systems, 30(1-7):107-117, 1998.

[26] K. M. Carley, J. Reminga and N. Kamneva. Destabilizing Terrorist Networks. NAACSOS Conference Proceedings, Pittsburgh, PA, 2003.

[27] L.C. Freeman. Centrality in social networks: Conceptual clarification. Social Networks 1:215239, 1979.

[28] P. Bonacich, P. Factoring and weighting, approaches to clique identification. Journal of Mathematical Sociology. 2, 113120, 1972.