Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Integrating relations and criminal background to identifying key individuals in crime networks

Fredy Troncoso[a,*], Richard Weber[b]

[a] Departamento de Ingeniería Industrial, Facultad de Ingeniería, Universidad del Bío- Bío, Concepción, Chile
[b] Departamento de Ingeniería Industrial, Facultad de Ciencias Físicas y Matemáticas, Universidad de Chile, Santiago, Chile

ARTICLE INFO

Keywords:
Crime analytics
Criminal groups
Social networks
Node evaluation
Human and social capital
Field theory

ABSTRACT

One of the most common methods used in the social network analysis of criminal groups is node importance evaluation, which focuses on the links between network members to identify likely crime suspects. Because such traditional node evaluators do not take full advantage of group members' individual criminal propensities, a new evaluator called the social network criminal suspect evaluator (*SNCSE*) is proposed. *SNCSE* incorporates members' individual criminal propensities into the node importance evaluation and employs a novel perspective based on concepts of human and social capital, an ego network structure, and an analogy between social interaction and field theory. SNCSE is applied to solve two real-world problems. Its effectiveness is compared with that of traditional evaluators. The results show that integrating criminal propensity into network analysis enables the more accurate identification of key suspects compared to alternative evaluators.

1. Introduction

Investigating individual and group criminality requires large quantities of resources and demands ever greater amounts of domain knowledge, skills, expertise, and time as criminal behavior becomes more sophisticated [35]. One way of increasing the efficiency and effectiveness of investigative work would be to improve the identification of individual suspects for any given crime. This would enable authorities responsible for public safety and crime prevention to better focus their scarce resources on the most likely candidates and drop their pursuit of the least likely candidates. The benefits could be particularly significant in cases where the initial population of possible suspects is large.

Criminal groups can be understood as social networks, implying that the traditional social network analysis (SNA) can be successfully used for their investigation. SNA extracts information from social networks using techniques such as node importance evaluation to identify key individuals and identify, for example, members of criminal groups. In traditional and non-traditional [36] [31] social network methods, the links between nodes are the main elements for analysis. However, additional information often exists on each member's propensity to commit certain types of offenses. The incorporation of this information in the techniques for the analysis of social networks could significantly enhance the effectiveness of investigative work [29]. The present study proposes a new approach for node evaluation that incorporates the criminal propensities of individual network members into the SNA of criminal groups. The study considers these propensities as well as links between nodes, generating results that provide better support for investigative work, particularly in criminal group analysis.

Section 2 of this article reviews the literature regarding applications of the social network approach to criminal group analysis, the tools this analysis traditionally uses, and the need for a new node importance evaluator that incorporates the criminal propensity of network members. Section 3 develops the newly proposed evaluator, discusses its theoretical basis, lays out the conditions for its application, and shows an example of its application. Section 4 applies the evaluator to two real-world datasets, showing its effectiveness. Finally, Section 5 presents the conclusions of this study and suggestions for future research.

2. Background

According to Wasserman [33], a social network can be defined as a set of nodes linked among each others, thus building pattern of relationships. Groups of criminals can be modeled by such networks where each offender is represented by a node and connections among

* Corresponding author.
E-mail addresses: ftroncos@ubiobio.cl (F. Troncoso), richard.weber@uchile.cl (R. Weber).

https://doi.org/10.1016/j.dss.2020.113405
Received 17 March 2020; Received in revised form 20 July 2020; Accepted 21 September 2020
Available online 25 September 2020
0167-9236/

them are displayed by arcs allowing the exchange of physical and/or non-physical resources [20]. Understanding criminals as part of a network rather than as individual units, opens a new perspective for crime investigation, at least for those kinds of delinquency that require the participation of various actors [18]. Using social network analysis (SNA) to analyze and explain the criminal group phenomenon is efficient and effective because the group members are involved in a process of social networking, both for the provisioning of illicit goods and services and the protection, regulation, and extortion of those involved in their provision and consumption [20].

Analyzing criminal groups in a social network context generally aims to identify criminal structures and/or key individuals based on the links between them. To this end, information from databases both public and private is utilized. The use of social network analysis to extract criminal intelligence has been used since 1991 [28] and widely employed, especially on published databases of terrorist groups since the attacks of September 11, 2001 [34] [23] [26] [14]. However, some kinds of criminal groups, such as terrorist cells and collusion networks, manipulate the relationships among their members, making their network very hard to represent and analyze [10].

In criminal investigative work using the social network approach, a key step is to establish a representative link between network members. This is very important to clearly define how the relationships among the members will be measured [6]. It requires that data describing human behavior garnered from diverse sources be properly modeled and transformed, which is one of the main problems arising in the spatio-temporal mining of social networks [7]. Human interactions are inherently multiplex with different types of relationships among the individuals which can lead to multilayers of information to consider [1]. Link analysis is the sub-area of SNA where such data are collected and used to establish links between nodes of the network [28] [9].

The relevant information could be found in many different sources being the principal approaches for link construction [15]:

- Self-report (establishes a link according to the declaration of each actor),
- Communication (establishes a link based on the interaction between individuals; e.g. money transfer or phone calls),
- Similarity, also called homophily (establishes a link based on the fact that individuals that are “close to each other” tend to be similar in their socio-demographic attributes and social behavior), and
- Co-occurrence (establishes a link between two individuals if they happened to spend time together at the same place; e.g. classmates at school or prison inmates).

An important approach used to extract information from social networks is node importance evaluation. It uses centrality measures [20] and node evaluation algorithms, all of which focus on links of the network. The most common centrality measures employed are the degree, closeness, betweenness, and eigenvector [19] [30], and the common algorithms are PageRank [22] and HITS [12]. In crime analysis, a node's importance is evaluated to identify particular structures within the network and its most important actors [8].

In addition to links, this study posits that information on network members' criminal background [5] should also be included as the propensity to belong to a criminal group (*Pcg*). Because this propensity is a node attribute, traditional node evaluators, which focus strictly on links, are not adequate for the task.

In light of the above and with the goal of achieving a more complete and effective analysis of criminal groups, the present study proposes a new node importance evaluator that considers the links between individuals as well as their respective propensities to belong to a criminal group. This approach provides an effective identification of the most important individuals in a crime network. The evaluator and the theoretical concepts that underpin it are formally introduced in the following section.

3. A novel evaluator including links and propensity to belong to a criminal group

The proposed new evaluator emerges from a novel perspective based on concepts borrowed from the theories of human and social capital, an analytic structure built around an ego network, and an analogy between the social interaction of individuals and the interactions of particles in field theory. It is this perspective that will enable the new evaluator to integrate links between individuals with their propensities to belong to a criminal group.

3.1. The novel evaluation approach - an overview

The ability of an individual to carry out a given economic activity can be determined by a set of attributes that reflect his or her acquisition of skills and knowledge over time. These attributes constitute the person's human capital, where the greater this capital, the more he or she will be able to identify and take advantage of economic opportunities [25]. Human capital has been the subject of studies from a variety of approaches and perspectives, much of them being conducted from a social perspective.

In the same way, an individual's ability to engage in a given criminal economic activity will depend on their human capital for committing certain types of offenses. This criminal human capital can be determined by some of the individual's attributes expressing his/her relevant knowledge and skills. If these attributes and the resulting criminal human capital can be somehow determined, an individual possessing a high level of human capital for a particular criminal activity can be readily classified as a strong suspect for past or present involvement in it.

Using the concept of group human capital, which measures the contribution of an individual to a criminal group, and more specifically to a gang, a microeconomic model of gang formation has been proposed in [4]. According to this model, a criminal group demands a certain minimum level of human capital from each of its members based on minimum required skills and a basic level of commitment to the group. By determining individuals' criminal group human capital, those with the highest levels of such capital can be classified as the individuals most likely to belong to a criminal group.

3.2. A representation for the criminal group human capital

An individual's social capital is determined by the set of contacts he/she maintains social relations via the respective links in a social network. This social capital must be considered when determining an individual's human capital because it is influenced by its contacts' human capital [3]. The criminal group human capital of an individual is thus determined by the criminal group human capital of those to which he/she is linked.

To express the criminal human capital, Hcg_i, we first define $G(N,A)$ as a graph representing a social network composed of a set N of nodes or individuals and a set A of arcs or links between the individuals. Then,

$$Hcg_i = Pcg_i + HCcg_i \ \forall \ i \in N \tag{1}$$

where.

- Pcg_i is the propensity of an individual i to belong to a criminal group without considering the contribution made by the other suspect network members to which individual is related. To obtain this value, we consider a set of attributes that measure the acquisition of knowledge and skills for some type of group crime. This value is given by

$$Pcg_i = r(S_i) \ \forall \ i \in N \tag{2}$$

in which S_i is the set of relevant attributes of individual i and r is some function, chosen under a certain context, that transforms this set into a

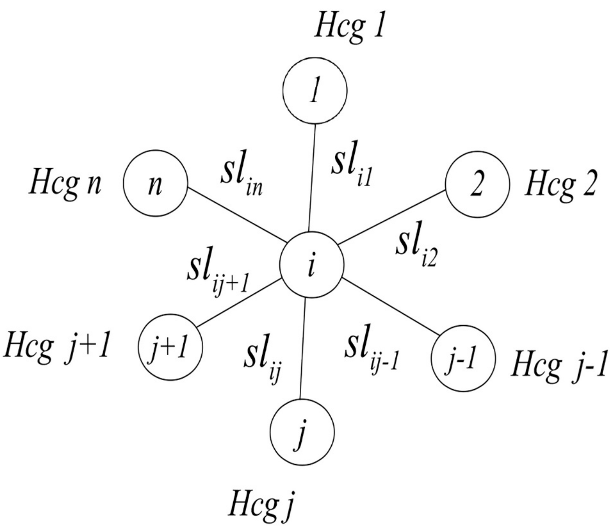

Fig. 1. Ego network of individual *i* for obtaining HCcg.

propensity value.

- $HCcg_i$ represents the criminal group human capital individual *i* receives from the individuals to which he/she is connected.

The contribution of others to an individual's human capital is a function of his/her social capital represented by the set of links to those with which he/she has relations. To define the function that will represent this contribution, we center the analysis on an ego network. In general, the ego network of an individual *i* is the network built with *i* at the center, known as *Ego*, and the set of individuals with whom *i* is directly related to, called *Alters*, as shown in Fig. 1.

In this ego network, the social capital of individual *i* (or Ego) is a function of his/her Alters' criminal human capital and of their links to *i*. Assuming that criminal group human capital is the desired characteristic and that this capital is transferred to *i* from the *Alters* through these links, the general function representing the contribution to *i*'s criminal group human capital is given by

$$HCcg_i = f(Hcg, sl)_{V_i} \;\; \forall\; i \in N \tag{3}$$

where *f* is a function that expresses the criminal group human capital transferred from the set of individuals $V_i \subset N$ to *i* via their social links *sl*. It is important that an appropriate form is adopted for this function so that a truly representative value for this transfer is obtained. In the next subsection, we present a key relationship for determining this form.

3.3. Social interaction and field theory: A key relationship

An appropriate form to represent the criminal group human capital must reflect the fact that the transfer of human capital from one individual to another depends on their link's strength. In other words, the stronger the link, the greater the amount of human capital that can be transferred [3].

The form finally chosen for the function was inspired by an analogy between social interaction among individuals and the interaction between particles described by field theory [13]. A similar analogy underlies certain node evaluation algorithms, which measure the topological potential of a node based on structural aspects of the network [21] [32] [16] [2]. According to field theory, every particle generates a field around itself that exerts a force or influence on every other particle located within its radius of action. Borrowing this idea, we assume that an individual's human capital exerts an influence on other individuals within his or her radius of action.

The potential of a particle *i* is expressed by the following Gaussian function:

$$\varphi(i) = \sum_{j=1}^{n} m_j e^{-\left(\frac{d_{ij}}{\sigma}\right)^2} \tag{4}$$

where *n* is the number of particles, m_j represents the mass of particle *j*, d_{ij} is the topological distance between particles *i* and *j*, and *σ* is a parameter that controls the particles' region of influence.

Using a Gaussian function such as in Eq. (4) to represent the transfer of human capital allows us to capture the fact that the interaction between individuals has local characteristics and that the human capital's influence decays as the link weakens.

Using Eq. (4), we propose the following function to represent individual *i*'s criminal group human capital:

$$HCcg_i = \sum_{j \in V} Hcg_j e^{-\left(\frac{d_{ij}}{\sigma}\right)^2}, \;\; \forall\; i \in N \tag{5}$$

where *σ* governs the region of influence over which a network member can contribute criminal group human capital to another member and d_{ij} represents the social distance between suspects *i* and *j*.

Given the properties of the Gaussian function, the region of influence of each node is approximately $3\sigma/\sqrt{2}$. When $\sigma \geq \sqrt{2}D/3$ (D is the diameter of the network), the influence region expands to the whole network [21]. Therefore $\sigma = \sqrt{2}D/3$ will be the value to which the parameter will be set.

It should be noted that the human capital transferred from individual *j* to individual *i* includes part of the human capital *j* received from individuals he/she is directly linked to but who are not necessarily directly linked to *i*.

Thus, the influence of individuals directly linked to *i* includes the influence of individuals not directly linked to *i*. In other words, the measurement of an individual's contribution to criminal group human capital indirectly takes into account the influence of all the individuals in the network.

3.4. Social network criminal suspect evaluator: The novel node evaluator

We now formally introduce our proposed new node importance evaluator that considers links and the propensity to belong to a criminal group, which we will call the social network criminal suspect evaluator (*SNCSE*). Substituting Eq. (5) into Eq. (1), we obtain

$$Hcg_i = r(S_i) + \sum_{j \in N} Hcg_j e^{-\left(\frac{d_{ij}}{\sigma}\right)^2} \;\; \forall\; i \in N \tag{6}$$

This can be written in matrix form as

$$(I - E)Hcg = R \tag{7}$$

where *I* is the identity matrix, *E* is a square matrix with elements $e^{-\left(\frac{d_{ij}}{\sigma}\right)^2} \geq 0 \; \forall i, j \in N$, *Hcg* is the column vector of elements $Hcg_i \; \forall\; i \in N$ and *H* is the column vector of elements $r(S_i) \geq 0$. To determine how the evaluator can be applied to a suspect network, observe first that it has the following form:

$$x_i = c_i + \sum_{j \in N} a_{ij} x_j \tag{8}$$

This form is a system of linear equations similar to the one used for solving Leontief's input-output model [17]. The Leontief input-output model is a quantitative economic technique that represents the interdependencies between different areas of a national economy or different regional economies. In that model, a_{ij} is interpreted as the input of product *i* per unit of output of *j*, x_i as the output of the emphith industry and c_i is the amount of the c_ith product in the bill of goods. The matrix form is

$$(I - A)X = C \tag{9}$$

where X and C are column vectors containing n components and A is the square matrix containing elements a_{ij}.

The input-output model assumes that the a_{ij} values are non-negative, as can be deduced from the definition of a product input and the postulate that each primary production process has only one output. The same is also true of the $e^{-\left(\frac{d_{ij}}{\sigma}\right)^2}$ values in Eq. (6), in which a single type of human capital (i.e., criminal group) is transferred to obtain a different level of the same type, and the minimum transferable amount from one individual to another is zero.

The main formal question in the input-output model is the existence of a static solution to the system of linear equations (Eq. (8)) that produces a bill of goods without negative outputs. Such a solution can be found if the corresponding dynamic system of product transfer is stable [27].

In a suspect network, a negative value for criminal group human capital has no meaning, as it would imply that, upon transferring part of his or her human capital, an individual becomes, in some sense, the opposite of suspect. In reality, of course, such a transfer can only make one individual less suspect than another. To ensure that the system of equations in Eq. (6) produces non-negative outputs, the dynamic system that transfers criminal group human capital between individuals must be stable. The level of human capital in this dynamic system is obtained via the following system of difference equations:

$$IHcg_{t+1} - EHcg_t = R \tag{10}$$

where t is a discrete-time criminal group human capital transference and a stable solution is reached when $Hcg_{(t+1)} = Hcg_t = Hcg$. This solution will represent the maximum criminal group human capital levels that can be attained in a sufficiently large amount of time. A solution for the system in Eq. (10) arrived at through iteration can be expressed as

$$Hcg_t = E^t Hcg_0 + (I + E + E^2 + ... + E^{t-1})R = E^t Hcg_0 + R\sum_{k=0}^{t-1} E^k \tag{11}$$

where the criminal group human capital converges to a stable value if and only if the absolute values of the eigenvalues λ_i of the matrix E are less than 1, that is, $|\lambda_i| < 1 \ \forall \ i \in N$ [27], in which case $I + E + E^2 + \dots$ converges to $(I - E)^{-1}$ and $E^t Hcg_0$ to the null matrix, and Hcg is obtained by $Hcg = (I - E)^{-1}R$.

If E is a nonnegative, indecomposable matrix, none of whose column sums is greater than one and whereby at least one of the column sums is less than one, then $|\lambda_i| < 1 \ \forall \ i \in N$ [27]. To guarantee this last condition, we divide the E matrix by the scale factor $\sum_{ij \in N} e^{-\left(\frac{d_{ij}}{\sigma}\right)^2}$. Thus, the *SNCSE* is

$$Hcg_i = r(S_i) + \frac{\sum_{j \in N} Hcg_j e^{-\left(\frac{d_{ij}}{\sigma}\right)^2}}{\sum_{ij \in N} e^{-\left(\frac{d_{ij}}{\sigma}\right)^2}} \ \forall \ i \in N \tag{12}$$

After obtaining the Hcg_i of each individual i of the network, those whose criminal group human capital increased the most with respect to their initial capital Pcg_i will be defined as the most important individuals. This increase is represented by the following:

$$\Delta Hcg_i = Hcg_i - r(S_i) \ \forall \ i \in N \tag{13}$$

3.5. Application to the example network

We will use an example network to show that the results of *SNCSE* are consistent with the results of the traditional node evaluator, and we explain the way it works. Fig. 2 shows our example network. This network has 12 nodes and 11 edges. All the edges have a value equal to 1.

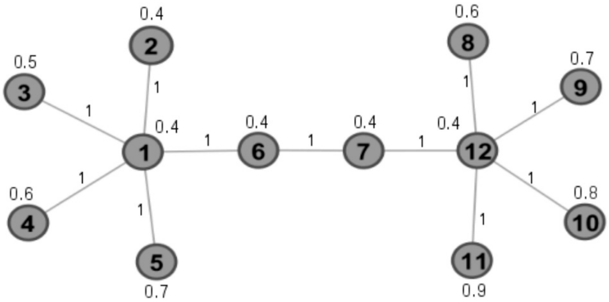

Fig. 2. Example network.

In the example network of Fig. 2, nodes 1, 6, 7 and 12 are the most important. These nodes must be identified as the most important in the network by any evaluator of node importance. Nodes 1 and 12 must have the same importance, and node 6 and node 7 must also have the same importance.

Table 1 shows the results of the application of centrality measures from SNA, the node evaluation algorithms, and the proposed evaluator: *SNCSE*.

In Table 1, the evaluators degree, betweenness, closeness, eigenvector, page rank, and hits and our proposed evaluator, *SNCSE*, identify nodes 1, 6, 7, and 12 as the most important in the network (in bold). These results show that the *SNCSE* is consistent with the results of traditional evaluators. However, *SNCSE* gave a different level of importance to nodes 1, 12, 6, and 7. This different level of importance is due to *Pcg*. Nodes 1 and 12 have the same level of *Pcg*, equal to 0.4. The sum of the *Pcg* of the neighbors of node 12 (7, 8, 9, 10, and 11) is 3.4. This sum is greater than the sum of *Pcg* of the neighbors of node 1 (2, 3, 4, 5, and 6), which is 2.4. For this reason, the criminal influence of the neighbors of node 12 is greater than the neighbors of node 1, and *SNCSE* better evaluates node 12 in that node 1 and node 12 become the best-evaluated nodes in the network. Nodes 6 and 7 have the same level of *Pcg*, equal to 0.4. Node 7 is closer to node 12 than node 6, and *SNCSE* evaluates node 7 as better than node 6. In general, each node on the right side (1, 2, 3, 4, 5, and 6) is closer to nodes with more *Pcg* than the nodes on the left side (7, 8, 9, 10, 11, and 12), and the *SNCSE* better evaluates the nodes on the right side than the equivalent nodes on the left side.

4. Applications of the social network criminal suspect evaluator

In the previous section, we introduced the *SNCSE* node evaluator, we analyzed the conditions for its application and applied the *SNCSE* to an example network. In this section, we present two applications and test *SNCSE* effectiveness. In the first application, the *SNCSE* is applied to identify members of a criminal group committing burglary in an uninhabited place. We used a dataset provided by the Crime Analysis Unit of the Public Prosecutor's Office of "Región del Biobío, Chile". In the second application, the *SNCSE* is applied to identify members whit the role of a leader in the Greek terrorist group November 17.

We propose the following generic methodology to apply SNCSE:

First, the network is established and social distances among nodes are determined. Next, we determine the propensity to belong to a criminal group (Pcg). Finally, we apply SNCSE to evaluate the nodes' importance.

In a particular application this methodology has to be adapted. The following subsections present particular applications providing ideas on how to apply the proposed evaluator SNCSE in different real-world cases.

Table 1
Results of evaluators applied to the network example.

Node	Degree	Betweenness	Closeness	Eigenvector	Page Rank	Hits	Pcg	Hcg	*SNCSE*(Δ*Hcg*)
1	**5**	**34**	**26**	**0.475**	**0.217**	**0.475**	**0.4**	**0.5245**	**0.1245**
2	1	0	36	0.199	0.049	0.199	0.4	0.4238	0.0238
3	1	0	36	0.199	0.049	0.199	0.5	0.5238	0.0238
4	1	0	36	0.199	0.049	0.199	0.6	0.6238	0.0238
5	1	0	36	0.199	0.049	0.199	0.7	0.7238	0.0238
6	**2**	**30**	**24**	**0.341**	**0.086**	**0.341**	**0.4**	**0.4441**	**0.0441**
7	**2**	**30**	**24**	**0.341**	**0.086**	**0.341**	**0.4**	**0.4457**	**0.0457**
8	1	0	36	0.199	0.049	0.199	0.6	0.6255	0.0255
9	1	0	36	0.199	0.049	0.199	0.7	0.7255	0.0255
10	1	0	36	0.199	0.049	0.199	0.8	0.8255	0.0255
11	1	0	36	0.199	0.049	0.199	0.9	0.9255	0.0255
12	**5**	**34**	**26**	**0.475**	**0.217**	**0.475**	**0.4**	**0.5613**	**0.1613**

4.1. Application to the public Prosecutor's office of "Región del Biobío, Chile" dataset

In order to show its usefulness for crime investigation, we applied *SNCSE* to a data set provided by the Crime Analysis Unit of the Public Prosecutor's Office of "Región del Biobío, Chile". This organization investigates crimes and conducts the corresponding actions in the south of Chile. The mentioned data set includes 1598 offenses committed between 2004 and 2017. Some registers of this set are shown in Table 2.

The columns in Table 2 have the following interpretation. "Cause Code" is the key to a criminal case investigated by the Crime Analysis Unit. It includes one or more suspects, labeled by the "Suspect Code", and one or more "Offenses". "Date" is the date on which the offense was committed.

In this subsection, *SNCSE* will be used to evaluate nodes considering their propensity to belong to a criminal group committing burglaries in an uninhabited place. This particular group has been investigated back in 2018 by the Crime Analysis Unit. As a result of this investigation, ground-truth information for each node is available.

4.1.1. Establish network and determine social distances

If two suspects have the same cause code, we connected them via a link since they acted together in at least one offense. Table 3 shows some examples of the number of criminal cases committed jointly by the suspects i and j (sl_{ij}), and their social distance (d_{ij}) obtained via Eq. (14).

$$d_{ij} = \frac{min\{sl_{ij} > 0 \ \ \forall\, i, j \in N\}}{sl_{ij}} \tag{14}$$

Fig. 3 shows the graph obtained where 77 nodes are linked via 374 arcs. Those suspects that have been identified by previous investigations as responsible for robbery in an uninhabited place are indicated by a circle.

4.1.2. Determine the propensity to belong to a criminal group (Pcg)

We assume that a suspect's previous criminal activities are relevant to estimate their propensity to belong to a criminal group (Pcg). Hence, we calculate two values for each suspect: the number of robberies between 2016 and 2017 (their recent experience) and the total number of such offenses during the observed period (their overall experience). Next, we compute the average and standard deviation for these two values over all 77 suspects.

Table 2
Subset of the database provided by the Crime Analysis Unit.

Cause Code	Suspect Code	Offense	Date
1200754382	TPGQ_36	Fighting in a Public Place	20-09-2012
1200756723	LRCJ_3	Burglary in an uninhabited place	11-09-2012
1200729201	AOJR_27	Injuries	02-09-2012
1200714814	JAQP_69	Injuries	25-08-2012
1200694081	HRVP_33	Drug possession	24-08-2012
1200678932	RUDQ_5	Injuries	19-08-2012
1200678866	PZLU_72	Criminal possession of a weapon	18-08-2012
1200653591	LPFU_18	Theft	10-08-2012
1200634593	SAPQ_22	Injuries	07-08-2012

Table 3
Relation between suspects.

Suspect *i*	Suspect *j*	sl_{ij}	d_{ij}
ABCD_32	EFGH_33	3	0.33
XBCQ_37	AFWP_41	1	1
RDEN_32	MOOA_86	1	1
PAPA_32	MAMA_32	1	1
PACG_3	AAAA_10	3	0.33
AIGD_13	JIAI_57	2	0.5

Fig. 4 displays the 77 suspects using the two dimensions mentioned before. The dotted lines next to the axes represent the average values of the respective axis. The other lines indicate the average values plus a standard deviation; thus leading to nine rectangles.

Suspects with highest overall experience and highest recent experience, i.e., those in the upper right rectangle, received $Pcg = 0.9$. The opposite case, i.e., the lower left rectangle (low level of experience and few current activities) is classified as $Pcg = 0.1$.

The other values of *Pcg* are determined following the practice applied at the Criminal Analysis Unit where the level of recent activities weighs more than the overall experience when it comes to estimate *Pcg*. The number next to the asterisks in each rectangle shown in Fig. 4 indicates the respective value of *Pcg*.

4.1.3. Apply SNCSE

Table 4 shows part of the results obtained by the application of the evaluators to the network of Fig. 4. The evaluators considered are the centrality measures from SNA (degree, betweenness, closeness, and eigenvector), the node evaluation algorithms (page rank and hits) and the proposed *SNCSE*. The table only shows the results for the members of the criminal group committing burglaries in an uninhabited place.

Table 4 shows the members sorted by their value from *SNCSE*. The leaders of the criminal band are marked with an asterisk (*).

The test of the effectiveness of *SNCSE* consisted of identifying the members of a criminal group committing burglaries in an uninhabited place into the first positions in the ranking generated by *SNCSE*. Then, we compared these results with the rankings generated by the SNA centrality measures and node evaluation algorithms. Table 5 shows the ranking of the 20 suspects with the highest evaluated indices by each evaluator.

Table 5 shows the members of the criminal group marked in bold and leaders marked by an asterisk (*). *SNCSE* identified more members of the criminal group than other evaluators (*SNCSE* 8 and the other evaluators 5). *SNCSE* concentrated more members in the first positions

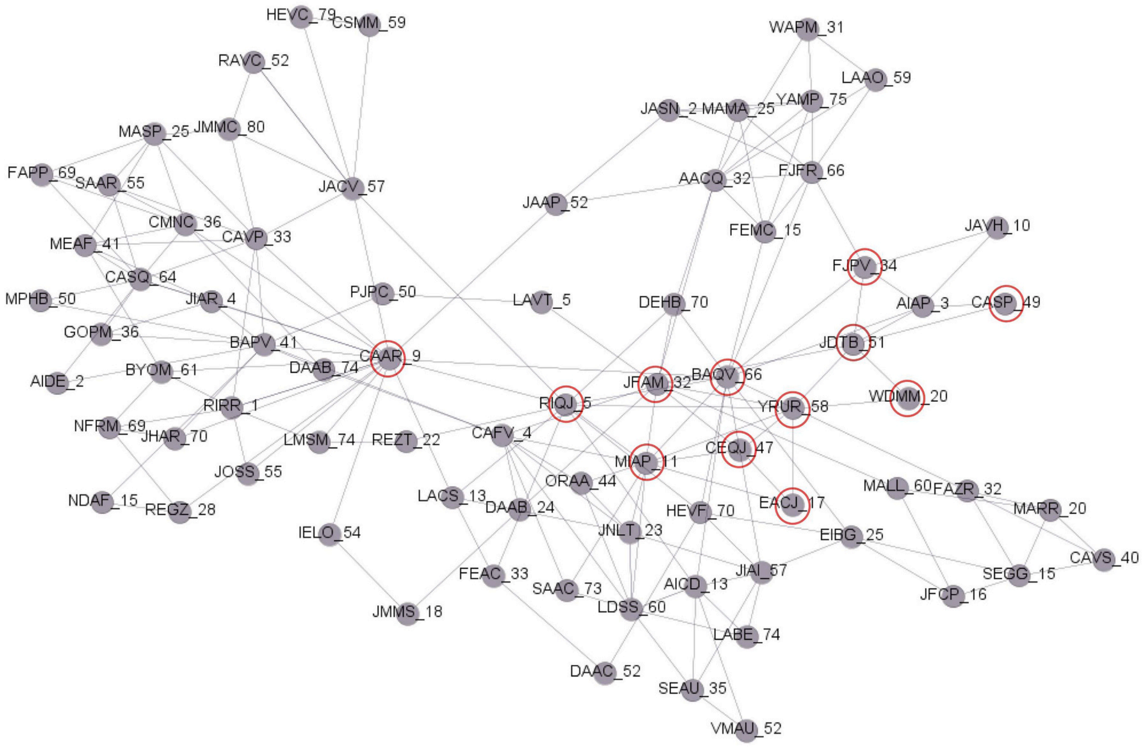

Fig. 3. Suspects network.

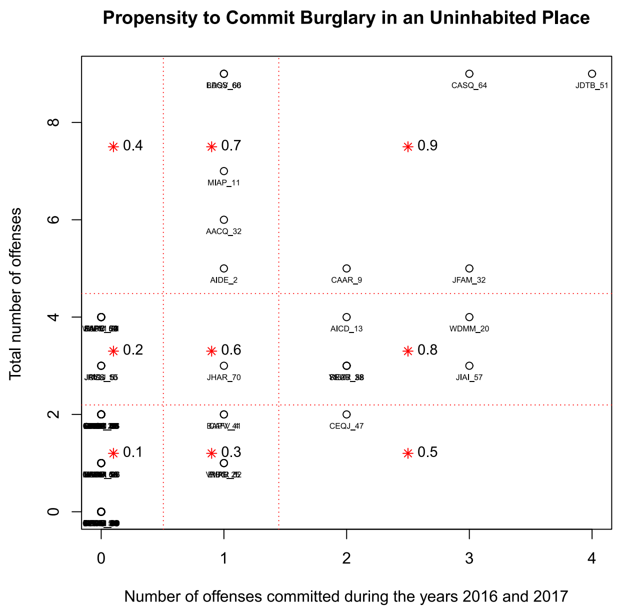

Fig. 4. Estimating the propensity to commit burglary in an uninhabited place.

and assigned a better place to the leaders.

Fig. 5 shows a comparison among *SNCSE* and the other evaluators. Each chart represents the percentage of members of a criminal group classified out of all suspects evaluated and ordered top to bottom.

In each chart of Fig. 5, an evaluator performed better than the others if its curve was nearest to the point (0,1). If the curve of an evaluator is nearer than another evaluator to this point, then the evaluator concentrates the members of the criminal group in the first positions of the ranking and identifies all the members “earlier”. *SNCSE* was able to include the group members “earlier” than the other evaluators, that is, it was able to concentrate the group members in the higher positions in the ranking.

In Eq. (15), we propose a performance measure for comparison of the evaluators in a quantitative manner.

$$\text{Performance} = \frac{\sum_{i \in N} y_i}{|N|} \tag{15}$$

where y_i is the percentage of members of the criminal group identified by the first i ranked suspects, i.e., the value that corresponds to member i on the curve of the respective evaluator in Fig. 5, and $|N|$ is the total number of ranked suspects.

Table 6 shows the performance of each evaluator considered. As seen, *SNCSE* outperformed all other evaluators.

SNCSE considers that the suspects strongly linked to individuals with higher criminal propensity may be associate with a criminal group. This fact can lead to a False Positive (a suspect identified as a member of a group when it is not). Such a False Positive delays the criminal investigative process since investigative resources are spent unnecessarily. However, a False Negative (a suspect identified as not being a member of a criminal group when in reality it is) is generally more relevant than a False Positive given the social cost associated.

Fig. 6 shows False Positive Rates (FPR, triangles) and False Negative Rates (FNR, Circles) for the two best evaluators (*SNCSE* and Betweenness) and the mean values of these rates considering all the evaluators, for six different rankings of suspects. As can be seen, SNCSE outperforms consistently the alternative evaluators for FPR as well as for FNR, respectively. The *SNCSE* has False Negative Rates lower than the False Positive Rates for all rankings except for the ranking 10.

4.2. Application to the network of the Greek terrorist group November 17

The revolutionary organization November 17 (N17) [24] was founded following the violent suppression of student protests at the Athens Polytechnic School by security forces of the Greek military junta in November 1973. N17 was a Marxist-Leninist group opposed to capitalism, imperialism, and the military. N17 have attacked a variety of targets since 1975, using assassination and bombing. The frequency of attacks has not been high, with the group being reliant on stolen

Table 4
Results of evaluators for each of the key suspects.

Suspect	Degree	Betweenness	Closeness	Eigenvector	PageRank	Hits	SNCSE
JFAM_32*	13	559.278	181	0.228	0.033882245	0.03195465	0.01515586
CAAR_9	18	1147.43	156	0.27	0.047489832	0.056184881	0.012817484
RIQJ_5	9	218.711	178	0.255	0.018858344	0.034209921	0.011789292
LDSS_60	9	51.76	232	0.245	0.014519162	0.015022989	0.011402661
BAQV_66*	11	684.414	163	0.257	0.027518859	0.038799971	0.01135948
MIAP_11	10	141.676	191	0.307	0.018384241	0.027499563	0.011125503
JIAI_57	9	162.551	215	0.196	0.020166234	0.017267781	0.01059808
AICD_13	8	64.753	223	0.232	0.01333435	0.016132859	0.010379399
DEHB_70	6	65.7	200	0.158	0.014296928	0.025553392	0.00890763
VMAU_52	4	0	264	0.111	0.007196447	0.004325847	0.008604627
YRUR_58	5	41.732	249	0.057	0.013776418	0.008310711	0.008498517
BAPV_41	11	359.606	187	0.13	0.029172162	0.026457822	0.008447545

weapons and material to conduct its operations. The last attack that the group is known to have undertaken was the assassination of the British Defense Attaché to Athens, Brigadier Saunders, in June 2000. Following a botched bombing attempt in 2002, in which group member Savas Xiros was injured and subsequently arrested, abundant information about the organization and structure of N17 was released into the public domain. It is believed, but not confirmed, that N17 no longer exists in a form that is capable of conducting terrorist operations.

In this section, we present the application of the proposed *SNCSE* to identify members with the role of "Leader" using the available N17 dataset. We take the data generated by a previous study [24] [11] as input for our analysis. Eight of 22 terrorists in the network were identified as Leaders.

Table 7 shows the resources that each member of N17 controlling, its faction, and its role in the group. Table 7 also shows the abbreviated name in () and the * indicate the members with leader role.

4.2.1. Network and determination of distances

Using news summaries and trial reports, the network was obtained by [11] and is shown in Fig. 7; see also [24]. Our analysis is based on this network.

Next, we have to establish the distances d_{ij} among individuals in the N17 network. We determine these distances based on the factions that the members belong to; see Table 7.

The main factions are: 1st Generation Founders (G), the Sardanopoulos faction (S), and the Koufontinas faction (K).

On the basis of these factions, we establish the respective distances as shown in Eq. 16

$$d_{ij} = \begin{cases} 0.25 & \text{if terrorists } i \text{ and } j \text{ belong to the same faction} \\ 0.5 & \text{if terrorists } i \text{ and } j \text{ belong to different factions} \\ 0.75 & \quad \text{if } i \text{ or } j \text{ does not belong to any faction} \end{cases} \tag{16}$$

4.2.2. Determination of Pcg

In this case, Pcg represents the propensity of a member to take the role of a leader in the terrorist organization. To determine Pcg, we propose a simple score based on the relation between each attribute shown in Table 7 and the role.

Prior to establish this score, we simplify the set of attributes by merging those that have identical distributions as will be shown next. As can be seen in Table 7, the attributes *Weapons* and *Safe houses* have identical columns and we selected *Weapons* as the representative attribute. The attributes *Drugs*, *Human trafficking*, and *Weapons smuggling* have the same distributions; we selected *Drugs* as the representative attribute. Similarly, the attributes *Bank robberies* and *Stealing weapons* have the same distribution; we selected *Bank robberies* as the representative attribute. The attribute *Attacks* takes the same value for all terrorists and is discarded from the analysis. Thus, the attributes considered in determining the capability of being a leader are *Money*, *Weapons*, *Drugs*, and *Bank robberies*.

Having simplified the attribute set, we now use the information gain

Table 5
Ranking of suspects generated by each evaluator.

Ranking	Degree	Betweenness	Closeness	Eigenvector	PageRank	Hits	SNCSE
1	**CAAR_9**	**CAAR_9**	**CAAR_9**	**MIAP_11**	**CAAR_9**	**CAAR_9**	**JFAM_32***
2	**JFAM_32***	**BAQV_66***	**BAQV_66***	**CAAR_9**	**JFAM_32***	**BAQV_66***	**CAAR_9**
3	BAPV_41	**JFAM_32***	**RIQJ_5**	**BAQV_66***	BAPV_41	**RIQJ_5**	**RIQJ_5**
4	**BAQV_66***	BAPV_41	**JFAM_32***	**RIQJ_5**	**BAQV_66***	FJFR_66	LDSS_60
5	AACQ_32	CAFV_4	BAPV_41	LDSS_60	CAFV_4	**JFAM_32***	**BAQV_66***
6	**MIAP_11**	JACV_57	MALL_60	AICD_13	CASQ_64	AACQ_32	**MIAP_11**
7	CAFV_4	MALL_60	**MIAP_11**	ORAA_44	JIAI_57	**MIAP_11**	JIAI_57
8	JIAI_57	**RIQJ_5**	CAFV_4	**JFAM_32***	AACQ_32	FEMC_15	AICD_13
9	LDSS_60	FJFR_66	LACS_13	CAFV_4	SAAR_55	LACS_13	DEHB_70
10	**RIQJ_5**	AIAP_3	DEHB_70	JIAI_57	**RIQJ_5**	CAFV_4	VMAU_52
11	AICD_13	JIAI_57	FJFR_66	JNLT_23	RIRR_1	BAPV_41	**YRUR_58**
12	CASQ_64	CASQ_64	JIAR_4	LACS_13	**MIAP_11**	DEHB_70	BAPV_41
13	FJFR_66	AACQ_32	JACV_57	AACQ_32	FJFR_66	JASN_2	CAFV_4
14	CAVP_33	**MIAP_11**	HEVF_70	DEHB_70	ORAA_44	ORAA_44	JNLT_23
15	FEMC_15	LACS_13	CASQ_64	FJFR_66	SEGG_15	YAMP_75	ORAA_44
16	ORAA_44	CAVP_33	JAAP_52	SAAC_73	LACS_13	CASQ_64	SEAU_35
17	RIRR_1	RIRR_1	JIAI_57	BAPV_41	FEMC_15	JIAR_4	**JDTB_51**
18	SAAR_55	CMNC_36	RIRR_1	FEMC_15	JIAR_4	MAMA_25	**WDMM_20**
19	DEHB_70	HEVF_70	JHAR_70	SEAU_35	MASP_25	MALL_60	LACS_13
20	JACV_57	FEMC_15	AACQ_32	HEVF_70	MALL_60	JIAI_57	HEVF_70

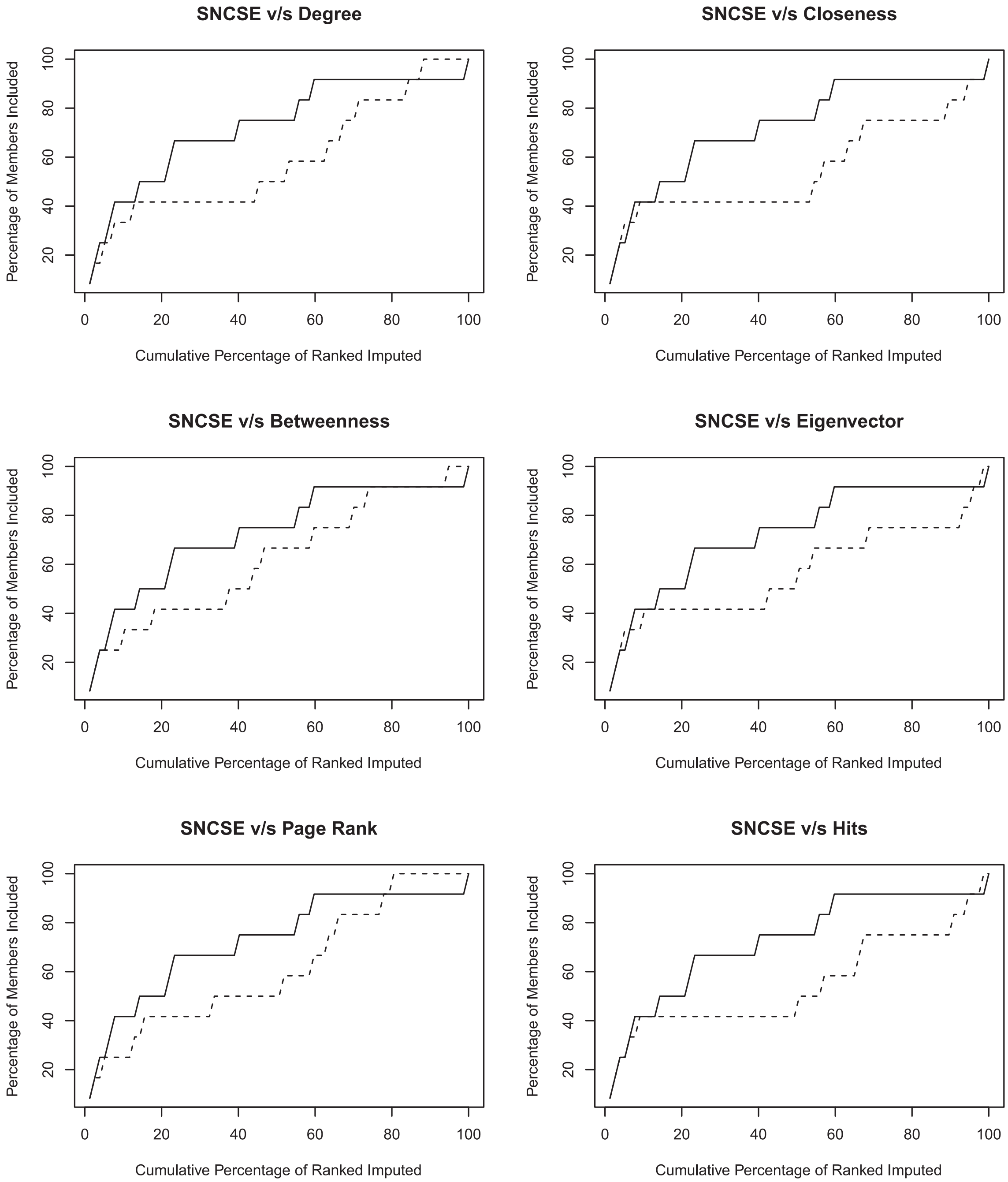

Fig. 5. Effectiveness test: Inclusion of members of a criminal group committing burglaries in an uninhabited place.

Table 6
Performance of each evaluator considered.

Evaluator	*Performance*
SNCSE	0.7316
Betweenness	0.6266
Page Rank	0.6201
Degree	0.5931
Eigenvector	0.5725
Closeness	0.5552
Hits	0.5552

criterion to establish the relation between each one of the remaining attributes and the role. An attribute's information gain is defined as the difference between the prior uncertainty and expected posterior uncertainty using the attribute. This measure determines the part of information contained in each attribute that will help us to characterize the role. The values are shown in Table 8.

The Pcg function for each member of the group is represented by Eq. 17:

$$Pcg_i = 1 - \sum_k P_k S_{ki} \tag{17}$$

where P_k is the normalized value of information contained in the attribute k and S_{ki} is the value (1 or 0) of the attribute k for the member i. Fig. 8 shows the Pcg level of each member of the terrorist group.

As expected, Fig. 8 shows that the individuals with the highest Pcg are the leaders except two: 6-Dimitris Koufontinas (DK*) and 3-Christodoulos Xiros (CX*). The analysis of the *SNCSE* application will focus mainly on the eight leaders.

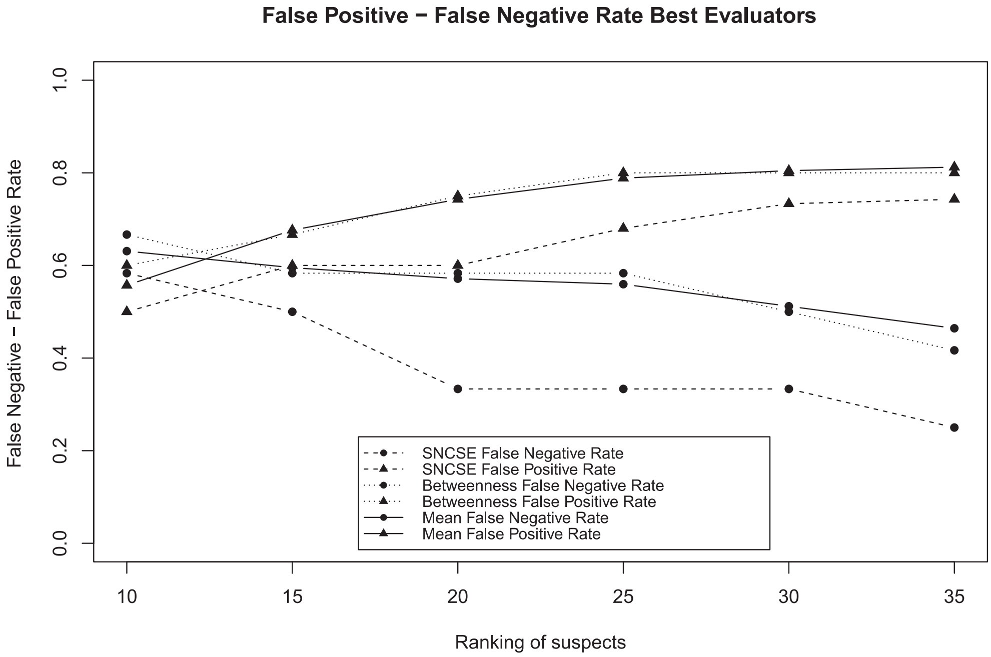

Fig. 6. False Positive - False Negative Rate of two best evaluators and Mean Rates.

4.2.3. *Apply SNCSE*

Table 9 shows the results obtained by the evaluators applied to the network of Fig. 4 and the performance of each evaluator according to Eq. (15). Table 9 is organized by descending order of *SNCSE*.

Table 9 shows the good performance obtained by the evaluators except for Betweenness. *SNCSE* achieves the best performance closely followed by Hits and Degree. Despite the low Pcg level of the leaders 6-Dimitris Koufontinas (DK *) and 3-Christodoulos Xiros (CX *), *SNCSE* ranks them within the first nine positions as shown in Fig. 8.

Table 10 shows that traditional evaluators rank 3-Christodoulos Xiros (CX*) among the first four places and 6-Dimitris Koufontinas (DK*) among the first five places. That is, given their role as leaders, they get a key position in the network. This key position is used by *SNCSE* and assign 3-Christodoulos Xiros (CX*) and 6-Dimitris Koufontinas (DK*) a better position than the operational members (except 15-Savas Xiros (SX)), despite their low Pcg.

As Fig. 8 reveals, the members 4-Constantinos Karatsolis (CK), 9-Iraklis Kostaris (IK), 12-Patroclos Tselentis (PT), and 18-Thomas Serifis (TS) have a medium level of Pcg. Table 10 shows through the traditional evaluators that these members do not have a key position in the network. Therefore, *SNCSE* dismisses them as leaders.

Fig. 9 compares *SNCSE* to the other evaluators and its analysis is similar to the one in Fig. 5 in subsection 4.1.3. The y-axis of each chart represents the percentage of leaders of the Greek terrorist group November 17 identified out of all members evaluated. The x-axis represents all group members ordered from top to bottom according to the respective evaluator. *SNCSE* concentrates more leaders in the first positions than all other evaluators. If we consider a ranking of eight

Table 7
Resource control, Role, and Faction in the Greek terrorist group November 17.

Name	Money	Weapons	Safe	Attacks	Drugs	Human	Weapons	Bank	Stealing	Faction	Role
			houses			trafficking	smuggling	robberies	weapons		
1-**Alexandros Giotopoulos (AG*)**	1	0	0	1	0	0	0	1	1	G	Leader
2-**Anna (An*)**	0	0	0	1	0	0	0	0	0	G	Leader
3-**Christodoulos Xiros (CX*)**	0	1	1	1	0	0	0	1	1	K	Leader
4-Constantinos Karatsolis (CK)	0	1	1	1	1	1	1	0	0	S	Operational
5-Constantinos Telios (CT)	0	1	1	1	0	0	0	1	1	K	Operational
6-**Dimitris Koufontinas (DK*)**	1	1	1	1	0	0	0	1	1	K	Leader
7-Dionysis Georgiadis (DG)	0	1	1	1	0	0	0	1	1	K	Operational
8-Elias Gaglias (EG)	0	1	1	1	0	0	0	1	1	K	Operational
9-Iraklis Kostaris (IK)	0	1	1	1	1	1	1	0	0	S	Operational
10-**Nikitas (Ni*)**	0	0	0	1	0	0	0	0	0	G	Leader
11-Ojurk Hanuz (OH)	0	1	1	1	0	0	0	1	1	–	Operational
12-Patroclos Tselentis (PT)	0	1	1	1	1	1	1	0	0	S	Operational
13-**Pavlos Serifis (PS*)**	0	0	0	1	1	1	1	0	0	S	Leader
14-**Sardanopoulos (Sa*)**	1	0	0	1	1	1	1	0	0	S	Leader
15-Savas Xiros (SX)	0	1	1	1	0	0	0	1	1	K	Operational
16-Sotirios Kondylis (SK)	0	1	1	1	0	0	0	1	1	–	Operational
17-**Fotis (Fo*)**	0	0	0	1	0	0	0	0	0	G	Leader
18-Thomas Serifis (TS)	0	1	1	1	1	1	1	0	0	S	Operational
19-Vassilis Tzortzatos (VT)	0	1	1	1	0	0	0	1	1	K	Operational
20-Vassilis Xiros (VX)	0	1	1	1	0	0	0	1	1	K	Operational
21-Yiannis (Yi)	0	1	1	1	0	0	0	1	1	–	Operational
22-Yiannis Skandalis (YS)	0	1	1	1	0	0	0	1	1	–	Operational

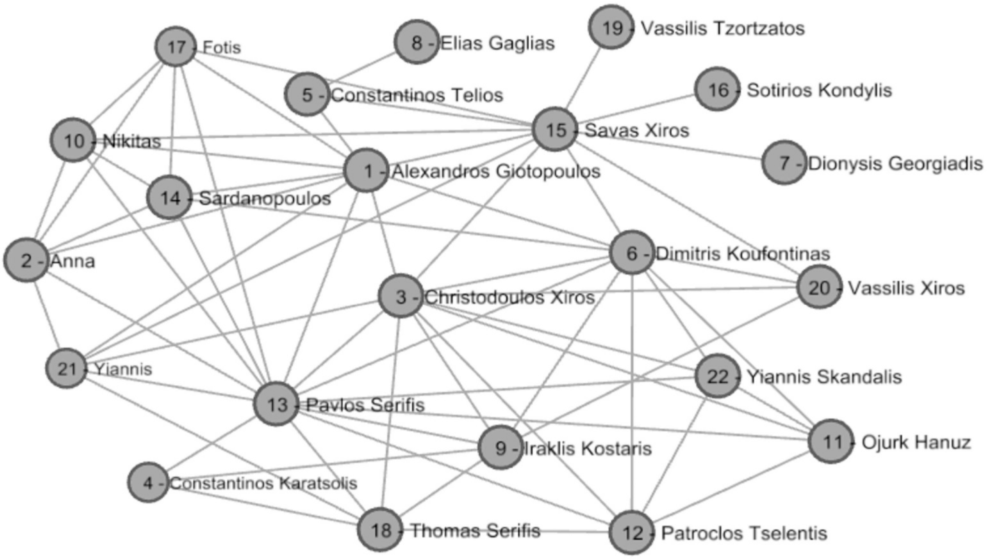

Fig. 7. Network of the Greek terrorist group November 17.

Table 8
Normalized information gain for each attribute.

Attribute	*Money*	*Weapons*	*Drugs*	*Bank robberies*
Value	0.2650	0.6409	0.0012	0.0928

members, equal to the number of leaders, SNCSE has only one false-positive (15-Savas Xiros (SX)) and only one false negative (3-Christodoulos Xiros (CX *)), the same number as Hits (see Table 10).

5. Conclusions and future research

An investigation of criminal groups requires that large quantities of resources be focused on key individuals to detect the existence of such groups or prevent their formation. By conceptualizing criminal groups as social networks, the identification of these individuals can be approached using node importance evaluators. This study proposed a novel evaluator called the *SNCSE*, which, in addition to network links, incorporates the propensity of each network member to belong to a criminal group toward achieving a more complete and effective analysis of criminal groups, thereby incorporating all available information.

SNCSE was applied to two real-world problems. The first application considered a dataset of suspects provided by the Public Prosecutor's Office of Región del Biobío-Chile. *SNCSE* outperformed alternative evaluators by identifying the most important nodes in the network. *SNCSE* included a greater number of members of a criminal group among the top-ranked suspects and positioned them higher within that ranking, therein considering the propensity of belonging to a criminal group (*Pcg*). This higher positioning of the members of a criminal group among the top-ranked individuals is an outcome that could have a significant positive impact on the short-term results of a criminal investigation and thus also on the efficient use of investigative resources. The False Positive and False Negative rates in *SNCSE* are lower than other evaluators, which leads to less delay in the criminal investigative process (less False Positives) and a lower social cost (less False Negatives). Additionally, because *SNCSE* incorporates social relations into its evaluations, the top-ranked suspects tend to be those who have the most significant network links. This fact suggests that the suspects

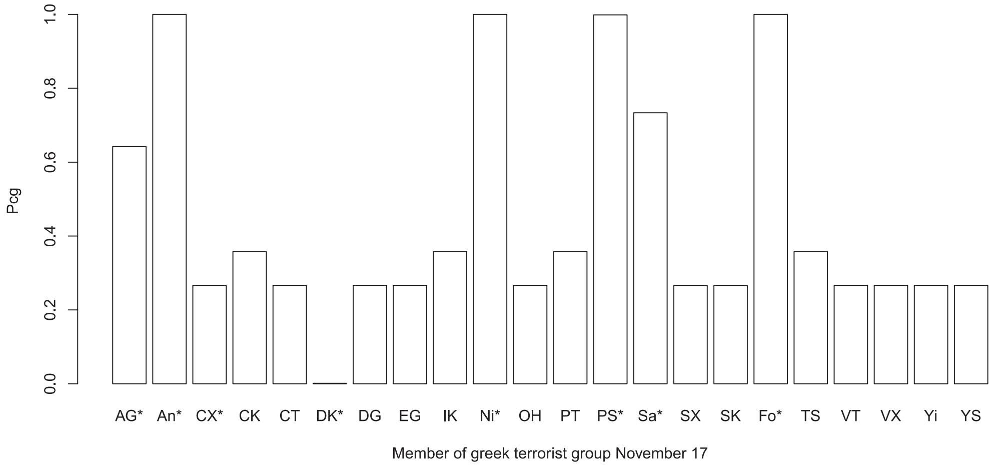

Fig. 8. Pcg of each member of the Greek terrorist group November 17.

Table 9
Results of evaluators for each member of the Greek terrorist group November 17.

Name	Degree	Betweenness	Closeness	Eigenvector	PageRank	Hits	SNCSE
13-Pavlos Serifis (PS*)	14	41.138	32	0.404	0.096269077	0.097432583	0.056837062
1-Alexandros Giotopoulos (AG*)	10	25.353	32	0.317	0.073880973	0.080972418	0.047085237
14-Sardanopoulos (Sa*)	6	0.924	40	0.215	0.043655781	0.057213798	0.038287937
2-Anna (An*)	6	0.833	41	0.204	0.047194061	0.056114225	0.037225992
6-Dimitris Koufontinas (DK*)	10	20.817	33	0.319	0.071133845	0.076903173	0.037212596
15-Savas Xiros (SX)	11	73.314	32	0.25	0.104142682	0.070114691	0.0371833
17-Fotis (Fo*)	6	3.121	37	0.207	0.050544048	0.061863212	0.0371424
10-Nikitas (Ni*)	6	3.121	37	0.207	0.050544048	0.061863212	0.0371424
3-Christodoulos Xiros (CX*)	11	23.814	32	0.342	0.074657644	0.07777342	0.034665621
21-Yiannis (Yi)	6	6.542	37	0.222	0.024447563	0.025742454	0.031620428
18-Thomas Serifis (TS)	6	2.977	42	0.192	0.051045426	0.053007751	0.02079457
9-Iraklis Kostaris (IK)	6	4.098	42	0.195	0.050538886	0.057009788	0.018059999
12-Patroclos Tselentis (PT)	6	0.917	42	0.212	0.042716851	0.047196148	0.017932102
11-Ojurk Hanuz (OH)	5	0	43	0.19	0.022090638	0.018807343	0.017253429
22-Yiannis Skandalis (YS)	5	0	43	0.19	0.022090638	0.018807343	0.017253429
4-Constantinos Karatsolis (CK)	3	0	49	0.103	0.032270328	0.036794374	0.013208241
5-Constantinos Telios (CT)	3	20	45	0.075	0.039143434	0.022725228	0.009663123
20-Vassilis Xiros (VX)	4	2.03	40	0.143	0.040051405	0.046611113	0.007686253
16-Sotirios Kondylis (SK)	1	0	52	0.032	0.010223008	0.004145296	0.002548613
19-Vassilis Tzortzatos (VT)	1	0	52	0.032	0.01703266	0.012435887	0.002214273
7-Dionysis Georgiadis (DG)	1	0	52	0.032	0.01703266	0.012435887	0.002214273
8-Elias Gaglias (EG)	1	0	65	0.01	0.019294346	0.004030658	0.002013481
Performance	0.801136	0.698863	0.761363	0.778409	0.761363	0.812500	0.823863

Table 10
Ranking of members generated by each evaluator.

Ranking	Degree	Betweenness	Closeness	Eigenvector	PageRank	Hits	SNCSE
1	**PS***	SX	SX	**PS***	SX	**PS***	**PS***
2	**CX***	**PS***	**PS***	**CX***	**PS***	**AG***	**AG***
3	SX	**AG***	**AG***	**DK***	**CX***	**CX***	**Sa***
4	**AG***	**CX***	**CX***	**AG***	**AG***	**DK***	**An***
5	**DK***	**DK***	**DK***	SX	**DK***	SX	**DK***
6	**An***	CT	Yi	Yi	TS	**Ni***	SX
7	IK	Yi	**Ni***	**Sa***	**Ni***	**Fo***	**Fo***
8	**Ni***	IK	**Fo***	PT	**Fo***	**Sa***	**Ni***
9	PT	**Ni***	VX	**Ni***	IK	IK	**CX***
10	**Sa***	**Fo***	**Sa***	**Fo***	**An***	**An***	Yi
11	**Fo***	TS	**An***	**An***	**Sa***	TS	TS
12	TS	VX	IK	IK	PT	PT	IK
13	Yi	**Sa***	TS	TS	VX	VX	PT
14	OH	PT	PT	OH	CT	CK	OH
15	YS	**An***	OH	YS	CK	Yi	YS
16	VX	OH	YS	VX	Yi	CT	CK
17	CK	YS	CT	CK	OH	OH	CT
18	CT	CK	CK	CT	YS	YS	VX
19	DG	DG	DG	DG	EG	DG	SK
20	EG	EG	SK	SK	DG	VT	VT
21	SK	SK	VT	VT	VT	SK	DG
22	VT	VT	EG	EG	SK	EG	EG

who are linked to such individuals may also be associated with criminal groups. Sub-networks consisting of the highest-ranked individuals' ego networks could, therefore, be used as a base for broadening criminal group investigations.

The second application considered a public dataset of the Greek terrorist group November 17. This application proves that the *SNCSE* identifies effectively key individuals with an apparent low propensity and with a key position in the network. The *SNCSE* also underestimated effectively the importance of individuals with a medium propensity and without a key position in the network.

Regarding future research, the following extensions are of particular interest:

- Developing a methodology to detect communities in the sub-networks constituting the ego networks of each of the *n* highest-ranked suspects. This would strengthen efforts to identify criminal groups.
- Incorporating the propensities to various types of group crimes into the newly proposed evaluator. This would enrich the information used in the node evaluation.
- Using available information such as criminal causes, offenses, date of the offenses, frequency of offenses, convictions, age, and sex, among others. Advanced machine learning techniques may be employed to better estimate *Pcg* based on the before-mentioned information.

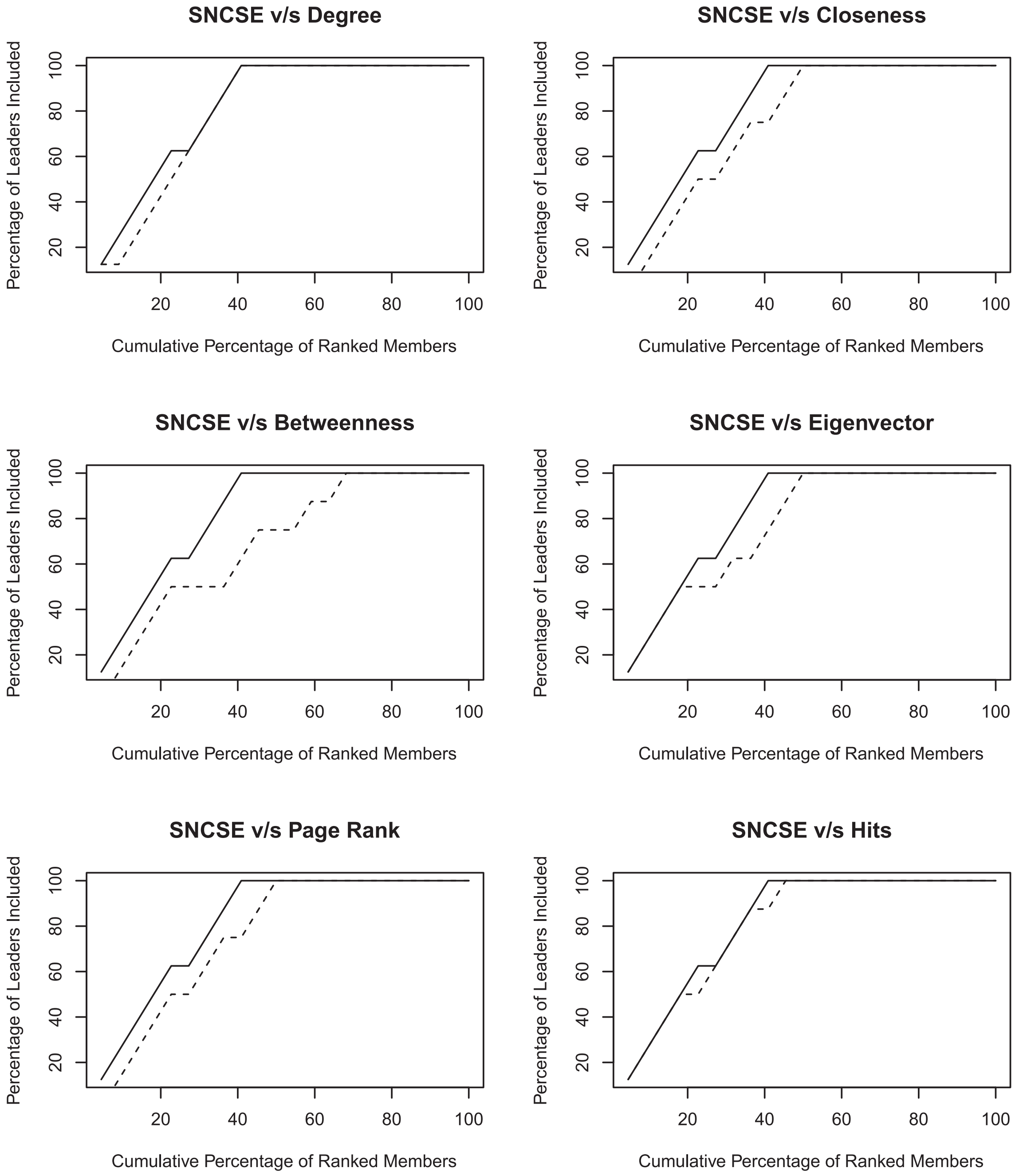

Fig. 9. Effectiveness test: Identification of leader role in the Greek terrorist group November 17.

Acknowledgments

The authors gratefully acknowledge the support of the Santiago-based Complex Engineering Systems Institute (CONICYT PIA/BASAL AFB180003), the Anillo projectACT87 "Quantitative methods in security", FONDEF project ID20I10230ANID and the Ph.D. program in Engineering Systems at the Universidad de Chile. The first author was the recipient of a CONICYT grant number 21120226 to pursue doctoral studies in Engineering Systems at the Universidad de Chile. The first author acknowledges the Criminal Analysis Unit of the Public Prosecutor's Office of Región del Biobío-Chile for the technical support and providing the dataset under a collaboration and internship agreement. The first author also acknowledges the financial support of Universidad del Bío-Bío by the Initiation Research Project2060204IF/I and Macro Facultad de Ingeniería by the ProjectING 2030 I + D 20-34. The second author acknowledges financial support by FONDEF project ID16I10222 CONICYT.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.dss.2020.113405.

References

[1] P.V. Bindu, P. Santhi Thilagam, Deepesh Ahuja, Discovering suspicious behavior in multilayer social networks, Comput. Hum. Behav. 73 (2017) 568–582.

[2] Qing Cheng, Jincai Huang, Zhong Liu, Cheng Zhu, Evaluation method of effect from network attack considering node multi-property feature, Mechatronic Science, Electric Engineering and Computer (MEC), 2011 International Conference on, pages 1947–1952, IEEE, 2011.

[3] James S. Coleman, Social capital in the creation of human capital, Am. J. Sociol.

(1988) S95–S120.
[4] W. Antony, Dnes and Nuno Garoupa. Behavior, human capital and the formation of gangs, Kyklos 63 (4) (2010) 517–529.
[5] Troncoso Espinosa Fredy Humberto, Prediction of recidivism in thefts and burglaries using machine learning, Indian J. Sci. Technol. 13 (06) (2020) 696–711, https://doi.org/10.17485/ijst/2020/v13i06/149853 ISSN 0950–7051.
[6] Katherine Faust, George E. Tita, Social networks and crime: pitfalls and promises for advancing the field, Ann. Rev. Criminol. 2 (1) (2019) 99–122.
[7] Lise Getoor, Christopher P. Diehl, Link mining: a survey, ACM SIGKDD Explor. Newslett. 7 (2) (2005) 3–12.
[8] R. Grassi, F. Calderoni, M. Bianchi, A. Torriero, Betweenness to assess leaders in criminal networks: New evidence using the dual projection approach, Soc. Networks 56 (2019) 23–32.
[9] R.V. Hauck, H. Atabakhsb, P. Ongvasith, H. Gupta, Hsinchun Chen, Using coplink to analyze criminal-justice data, Computer 35 (3) (2002) 30–37 Mar.
[10] Brian Hayes, Computing science: connecting the dots, Am. Sci. 94 (5) (2006) 400–404.
[11] C. Irwin, C. Roberts, N. Mee, Counter terrorism overseas, Dstl Report, Dstl/CD053271/1.1, 2002.
[12] Jon M. Kleinberg, Authoritative sources in a hyperlinked environment, J. ACM 46 (5) (September 1999) 604–632 (ISSN 0004-5411).
[13] L. Lev Davidovich Landau, E. Evgenii Mikhailovich Lifshits, The Classical Theory of Fields, volume 2, Butterworth-Heinemann, 1975.
[14] Mark A. Lauchs, Robyn L. Keast, Vy Le, Social network analysis of terrorist networks: can it add value? Pak. J. Criminol. 3 (3) (2012) 21–32.
[15] Hady W. Lauw, Ee-Peng Lim, Hweehwa Pang, Teck-Tim Tan, Social network discovery by mining spatio-temporal events, Comput. Math. Org. Theory 11 (2) (2005) 97–118.
[16] Lv Le, Hewei Yu, A new method for evaluating node importance in complex networks based on data field theory, Networking and Distributed Computing (ICNDC), 2010 First International Conference on, pages 133–136, IEEE, 2010.
[17] Wassily Leontief, Input Output Economics, Oxford University Press, 1986.
[18] Jasmien Lismont, Eddy Cardinaels, Liesbeth Bruynseels, Sander De Groote, Bart Baesens, Wilfried Lemahieu, Jan Vanthienen, Predicting tax avoidance by means of social network analytics, Decis. Support. Syst. 108 (2018) 13–24.
[19] Jean Marie McGloin, David S. Kirk, Social network analysis, Handbook of Quantitative Criminology, pages 209–224, Springer, 2010.
[20] Jeffrey Scott McIllwain, Organized crime: A social network approach, Crime Law Soc. Chang. 32 (4) (1999) 301–323.
[21] Nan He, Gan Wen-Yan, et al., Evaluate nodes importance in the network using data field theory, Convergence Information Technology, 2007. International Conference on, pages 1225–1234, IEEE, 2007.
[22] Lawrence Page, Sergey Brin, Rajeev Motwani, Terry Winograd, The Pagerank Citation Ranking: Bringing order to the web. Technical Report 1999–66, Stanford InfoLab, 1999 November. (Previous number = SIDL-WP-1999-0120).
[23] Jialun Qin, Jennifer J. Xu, Daning Hu, Marc Sageman, Hsinchun Chen, Analyzing terrorist networks: A case study of the global salafi jihad network, Intelligence and Security Informatics, pages 287–304, Springer, 2005.
[24] C.J. Rhodes, E.M.J. Keefe, Social network topology: a bayesian approach, J. Oper. Res. Soc. 58 (12) (2007) 1605–1611.
[25] Theodore W. Schultz, Investment in human capital, Am. Econ. Rev. 51 (1) (1961) 1–17.
[26] Muhammad Akram Shaikh, Wang Jiaxin, Investigative data mining: Identifying key nodes in terrorist networks, Multitopic Conference, 2006. INMIC'06. IEEE, pages 201–206, IEEE, 2006.
[27] Robert Solow, On the structure of linear models, Econometrica (1952) 29–46.
[28] Malcolm K. Sparrow, The application of network analysis to criminal intelligence: An assessment of the prospects, Soc. Networks 13 (3) (1991) 251–274.
[29] Fredy Troncoso, Richard Weber, A novel approach to detect associations in criminal networks, Decis. Support. Syst. 128 (January 2020) 113–159, https://doi.org/10.1016/j.dss.2019.113159.
[30] Renée C. van der Hulst, Introduction to social network analysis (sna) as an investigative tool, Trends Org. Crime 12 (2) (2009) 101–121.
[31] Véronique Van Vlasselaer, Cristián Bravo, Olivier Caelen, Tina Eliassi-Rad, Leman Akoglu, Monique Snoeck, Bart Baesens, Apate: A novel approach for automated credit card transaction fraud detection using network-based extensions, Decis. Support. Syst. 75 (2015) 38–48.
[32] Teng Wang, Yanni Han, Wu. Jie, Evaluate nodes importance in directed network using topological potential, Information Engineering and Computer Science (ICIECS), 2010 2nd International Conference on, pages 1–4, IEEE, 2010.
[33] Stanley Wasserman, Social network analysis: Methods and applications, Volume 8, Cambridge university press, 1994.
[34] Jennifer Xu, Byron Marshall, Siddharth Kaza, Hsinchun Chen, Analyzing and visualizing criminal network dynamics: A case study, Intelligence and Security Informatics, pages 359–377, Springer, 2004.
[35] Jennifer J. Xu, Hsinchun Chen, Crimenet explorer: A framework for criminal network knowledge discovery, ACM Trans. Inf. Syst. 23 (2) (April 2005) 201–226 (ISSN 1046-8188).
[36] Ahmad Zareie, Amir Sheikhahmadi, Mahdi Jalili, Mohammad Sajjad Khaksar Fasaei, Finding influential nodes in social networks based on neighborhood correlation coefficient, Knowledge-Based Systems, page 105580, 2020 (ISSN 0950-7051).

Fredy Troncoso is Professor at the Department of Industrial Engineering of the Faculty of Engineering, Universidad del Bío-Bío, Chile since 2008. He is Industrial Engineer from University of Bío-Bío, Chile and holds a Phd. in Systems of Engineering, from University of Chile. Since 2014 he has been a professor of data mining in postgraduate courses and actively participates in applied research projects. His research interests include data mining, net mining, and artificial intelligence.

Richard Weber is Professor at the Department of Industrial Engineering of the Faculty of Physical and Mathematical Sciences, Universidad de Chile. From 1992 to 1998 he worked as data mining consultant for the company Management Intelligenter Technologien GmbH, Aachen in Germany before joining Universidad de Chile in 1999. Richard Weber was visiting professor at the University of Osaka in 1992, the University of Tokyo in 2003, the University of Alberta in 2006, **KU Leuven**, Belgium in 2013, University of Vienna in 2017, and Aachen University in Germany (2015, 2016, 2017, 2018, and 2019). His research interests include data mining, dynamic data mining, and computational intelligence. He is Associate Editor of the journals "Applied Soft Computing" and "Journal of the Operational Research Society" and serves on the editorial board of the journal "Intelligent Data Analysis". He is senior member of IEEE and member of ACM and INFORMS. Richard Weber holds a B.Sc. in Mathematics as well as a MS and a Ph.D., both in operations research, from Aachen University, Germany.