Online: ISSN 2645-2960; Print ISSN: 2141-3959

Detecting covert members: Quadrant approach for classification and identification of smart criminals

Abideen A. ISMAIL[a], Elizabeth, N. ONWUKA[a], Bala, A. SALIHU[a], Osichinaka C. UBADIKE[a,b]

a-Telecommunication Engineering Department, School of Electrical Engineering and Technology, Federal University of Technology, FUT Minna, Niger State.
b- Air Force Institute of Technology Kaduna
ismail.pg.610938@st.futminna.edu.ng, +2348102297219

Abstract

Telecommunication metadata is a resourceful tool that can be employed in fighting incessant crimes. One peculiar challenge in this resourceful material is the inability to access the personal status of criminal syndicate. It weakens evidence for identifying conspirators in crimes. Recently, quadrant approach has proven to be a better approach for analyzing metadata to unveil the level of involvement of the direct perpetrators. However, it was found that combination of only degree and betweenness centrality in this approach limits its ability to uncover the key-players, especially distant influencers. In this work, we have proposed an enhanced quadrant approach as a robust method for classifying criminal activities based on their relationships. The method reserves a portion of quadrants for identifying smart(hidden) criminals or fugitives. In order to ensure that all vital covert members are adequately uncovered, this study incorporates more social network analysis (SNA) metrics into the quadrant approach. It was found that using closeness centrality as a feature for strategic positioning make more conspirators become prominent than using betweenness centrality. Thus, the number of detected covert members was increased by detection of smart criminals in the quadrant. Out of four cases that were studied, the case where closeness centrality was combined with degree centrality detected 19.05% of conspirators among the criminal group as against the 2.38% of conspirators that were identified when betweenness and degree centrality were combined. The use of closeness centrality also reduced the inconspicuous conspirators to 59.52%.

Keywords: *Covert members; Affiliate criminals; Quadrant approach; Prominent; SNA metrics*

1. Introduction

The use of telecommunication devices has become ubiquitous (Catanese, Ferrara, & Fiumara, 2013). Criminals mostly make use of mobile phones on daily bases to mastermind their criminal activities and coverup their identities (Eiselt, H. A., & Bhadury 2015). Telecommunication metadata are collected remotely from the mobile devices like cellular phones and tablets. The collection of these vital information is usually unknown to end users and less suspicious by criminals compared to data gathered via surveillance devices. The metadata offers underlying information about transactions and relationships between any two actors, including time, duration, and frequency of their communication. Emergence of various techniques for analyzing relationships between two or more mobile phone users have made it possible to predict the tendencies and activities of the communicators. Investigations have revealed that human capital attribute and the social capital attribute are obtainable from Telecommunication Metadata (Bright, Greenhill, Britz, & Ritter, 2017).

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Organized crimes are found to be a coalition of individuals with different personalities (Keller, 2015). Security agencies should be concerned about identifying key members of criminal gangs. This is because identifying and apprehending the key players will jeopardize the coordination and operation of the criminals as others mostly depend on their masters for tricks and maneuvering in planning and executing criminal activities. Models for detecting important actors focus on the identification of key players (Gunnell, Hillier, & Blakeborough, 2016; Ortiz-arroyo, 2010).

Fighting criminal organizations require measures to identify strongholds and uncover hidden key-players of criminal syndicates. In an effort to fight incessant crimes, a number of strategies have been developed. Some of these are simulated using data on terrorist groups or drug trafficking organizations (DTO), a number of simulations experiments have been carried out using the DTO data. The strategies are directed towards identifying key players. Harvesting hidden key players is always a herculean task as they are difficult to identify. A key player in a criminal syndicate could be an actor with relatively low links (i.e., low number of direct contacts with fellow criminals), as it is known that some key players abstain from associating with ordinary criminals in order to safeguard their identities (Hulst, 2009). Hence, the need to go beyond communication data sometimes arise in the effort to determine the king players. Besides phone conversations, other activities such as bank transactions, traveling schedules, meetings and short message services (SMS) are considered as a source of data to broaden the systematic way of uncovering the key players.

One of the most feasible and informative techniques among several techniques that have been used to model the criminal activities is classification of the members of a syndicate using the role played by each member as the metric for grouping them, and thereafter establishing the relationship between the groups and individuals. These correlations help in determining the kernel of their planning and operations. It is reported that criminal activities are highly correlated with degree of centrality i.e. actively involved actors become more vulnerable to security intervention irrespective of their status. But, strategic positioning cannot be correlated with those identified as high-status members (Calderoni, 2012). The use of quadrant graph has proven to be a vital tool in analyzing multi-relational network. The Quadrant is deployed to identify those actors with high betweenness i.e. actors connecting one network layer with another one. With the quadrant technique, four layers are mapped out with different actors emerging as holders of strategic positions. They are key players because they are brokers of vital information (Grassi, Calderoni, Bianchi, & Torriero, 2019; Leuprecht, Aulthouse, & Walther, 2016).

In this study, we seek to investigate the effect of hidden roles on the vulnerability and strategic positioning of covert members (conspirators). Covert and overt members differ in their influences and capacities. Usually, highly influential covert members position themselves in such a way to evade detection. Strategic positioning is a hypothetic framework being used to classify fugitive criminals. Therefore, this work targets combination of four centrality metrics that can make conspirators become more vulnerable or move from the zone of less-suspicion (peripheral) to the zone of prominence.

The remaining parts of this paper are organized as follows: Section 2 discusses related works, methodology description and simulation is presented in section 3, section 4 presents simulation results and discuss, while section 5 concludes the paper.

2. Related Works

A number of researches in unveiling the hidden criminals have been proposed using Telecommunication Metadata.

The work of Bright *et al* (2017) reveals that a dichotomy that exists between the structural status and personal status when analyzing telecommunication metadata. The work investigates the effect of eliminating key actors from the point of view of using human capital attribute over the social capital attribute in network disruption. The work established that the use of human capital is more effective in disrupting criminal organizations than a social capital attribute. Similarly, Campana and Varese (2012), Varese, (2013) and Calderoni,(2012) worked towards harmonizing human capital and social capital status.

Researchers also focus on models for detecting key players, example includes the works of Gunnell *et al* (2016) and Ortiz-arroyo(2010). Kitsak *et al* (2010) investigated the effect of ascribing importance to all nodes that have high degree centrality and concludes that not all nodes with high degree centrality are key actors with respect to spreading capacity. Liu *et al*.,(2015) added that types of organizations and the structure dictates attributes to be used in identifying important actors. In addition, the work of Borgatti (2006) established that conventional metrics are ineffective in identifying the optimal set of key players. The work provided two definitions for identifying a set of key players in a network structure. The two definitions make use of structural attribute (social capital) to describe a set of key players.

The fight against criminal organizations had been hinging on how to identify strongholds in an organized criminal group (OCG) i.e., to uncover hidden key-player of an OCG (Qiao, Shan, & Zhou, 2017; Song, Zhou, Wang, & Xie, 2015). Personal attributes of members signifies the degree of impact on the growth and resilience of criminal organizations (Behzadan, Nourmohammadi, Gunes, & Yuksel, 2017). According to Lampe (2009), individual characteristics lend decorum in explaining the emergence and reshaping of criminal structure but unfortunately, crime data often exclude personal attributes of participants. It is asserted that implicit analysis of network can measure social skills of individual members that participated in a crime and those who do not show up under investigation (Lampe, 2009; Sparrow, 1991). Structural relationships had been used for identification of hidden features in the absence of real personal attributes of network entities (Hulst, 2009; Newman, 2002; Park, 2018).

A vast number of strategies have been evaluated using drug trafficking organization (DTO) data. These strategies are directed towards identifying key players, for example, Maeno and Ohsawa (2007) proposed a strategy that recognized an actor that appears in more than one segment of a particular crime data records. Also, the four aeroplanes used in the September 11 attacks in the US with the attackers represent four data records. An attacker that is found in another data record than his own is taken as an influencer i.e. key player (Maeno & Ohsawa, 2007). This method is considered to be heuristic for the identification of a key member in a terrorist group (Maeno, 2009). Maeno further developed the statistical inference method (SIM) to predict the highest order conspirator using the Global Jihad network data (Maeno, 2009). The SIM involved complex mathematical expressions. Yang, *et al*.,(2014) considered the SIM approach to be too unrealistic for real-life criminal scenarios.

It is a fact that a key player in criminal act could be an actor with relatively low links, as it is known that some key players abstain from associating with ordinary criminals in order to safeguard their identities (Hulst, 2009). Butt *et al* (2014) proposed a simple approach in identifying a set of key players by analyzing multi relationships among a suspected criminal group. The Multi relationships includes phone conversations, bank transactions, record of air travels, meetings and short message services (SMS) each of which serve as a network so that the multi-relationship constitute network layers. A key player is taking as an actor with the highest degree centrality from each network layer. Indeed, the method should be called harvester of hidden key players as they might be difficult to identify as significant actors if the analysis is done on a single network layer. However, this method is equally tedious to implement.

Morselli (2010) combined degree centrality and betweenness metric. The integration of these two fundamental social network analysis (SNA) metrics is conceived on the notion that degree centrality makes criminal actors vulnerable, while betweenness centrality can conceal an active criminal participator with very low participation (Bright, Greenhill, & Ritter, 2015; Morselli, 2009). With the betweenness metric, the strategic positioning of actors can be identified, by combing degree and betweenness centrality, Morselli tried to enhance the visibility of hidden key-players. Morselli (2010) also carved up this technique into a graph with four quadrants. Each quadrant hosts a set of actors according to their centrality metric values on the vertical and horizontal axes of the graph as shown in Figure 3. The method is used to find relationships between recorded activities of criminal gangs and their arrest using a scatter plot. Both the arrested criminals and those who were not arrested appeared in the four quadrants. The Quadrant makes obvious those that were arrested but could have ordinarily escape arrest. This technique is viewed as effective and less complex for practical purposes.

Calderoni (2010) also adopt the strategy of integrating centrality degree and betweenness metrics to find strategic positioning for actors in the drug trafficking organization (DTO) without resolving to scatter plot of nodes like the quadrant graph adopted in the work of Morselli (2010). The strategy is used to find a connection between the social capital status of participants in the drug business and their criminal activities. It is reported that criminal activities are highly correlated with degree centrality i.e. actively involved actors become more vulnerable to security intervention irrespective of their status. But, strategic positioning could not be correlated with those identified as high-status members (Calderoni, 2012). In the work of Gunnell et al. (2016), the multi-relational network is analyzed with the quadrant graph. The Quadrant is implored to identify those actors with high betweenness i.e., actors connecting one network layer with another one (they form the bridges between network layers). Four layers were examined in the work with different actors posing as holders of strategic position. They are key players because they are brokers of vital information (Grassi, Calderoni, Bianchi, & Torriero, 2019; Leuprecht, Aulthouse, & Walther, 2016).

The quadrant method has been implemented with good effect, however, so far, two SNA metrics were being considered. This work seeks to extend the work by Morselli (2010), by a pair-wise combination of four centrality measures viz: degree, betweenness, closeness and eigenvector centrality measures in order to achieve a more robust method of excavating hidden nodes in a criminal network. This is because the technique is less complex and is more apt to expose hidden key players in a criminal group.

3. Methodology

The methodology of carrying out this work is described in this section. The terminologies employed are also explained including the general concept of the quadrant method as it affects this work. Four cases were created for the purpose of our simulation and analysis. Due to non-access to telecommunications metadata for domestic criminal cases, data from the September, 11, 2001 US attack was employed in the simulation to test the method.

3.1 Simulation Setup

Figure 1 presents a flowchart depicting the method applied in this work. Dataset of the felons that masterminded 9/11, 2001 attacks, downloaded from UCINET website, were used. Structural relations among the participants were constructed from the dataset using Python anaconda 3.6, this is shown in figure 2. SNA metric tools were run on the simulated network structure to extract four basic centrality scores of all network participants. The extracted metrics include degree, betweenness, closeness, and eigenvector centrality. The next stage in the procedure according to figure 1 is the identification of the node's importance or relevancy. The decision block is to query the type of relevancy analysis approach intended. The left branch is for the single metric analysis; where only a single metric graph identifies a key-player in the structure, or a set of nodes with high scores are identified as a set of key players; i.e., influence maximization.

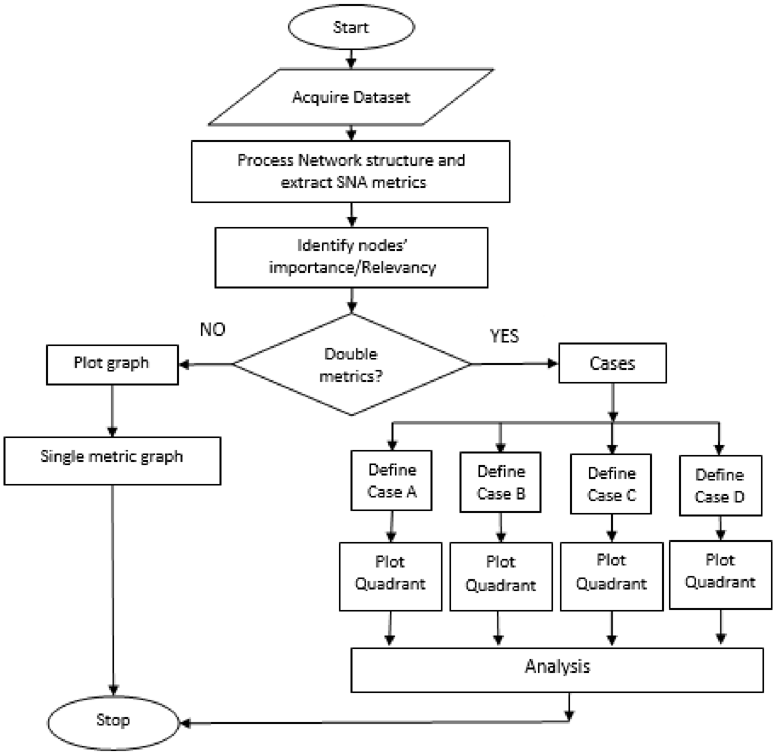

Figure 1: Flowchart of Methodology

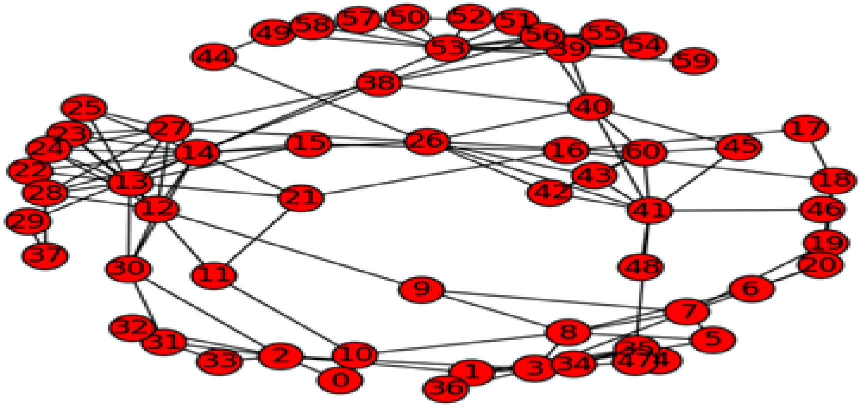

Figure 1: Anonymous Network structure of the September 11 attackers and conspirators

The right branch of the decision box points to relevancy evaluation of actors based on the quadrant approach i.e. partitioning of two overlapped metrics. The four SNA metrics extracted from the network structure of Figure 2 were paired to obtain four cases: A to D. Case A is a pair of degree and betweenness centrality metrics; case B is a pair of degree and closeness centrality metrics; case C is a pair of eigenvector and betweenness metrics; while case D is a pair of eigenvector centrality and closeness centrality metrics.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

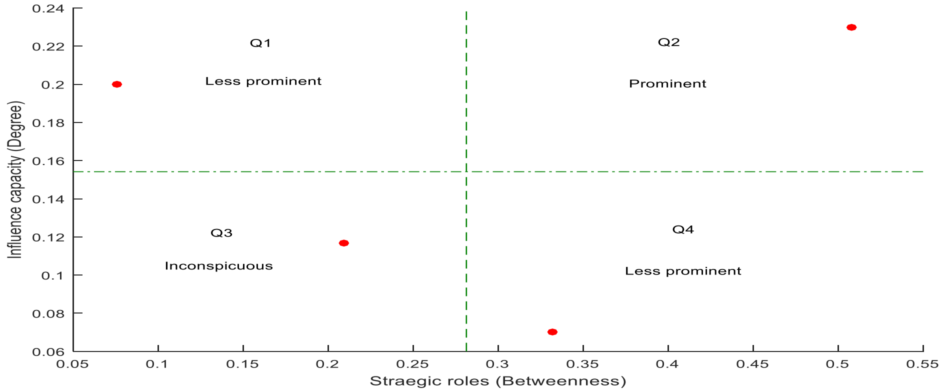

Figure 3: Typical Quadrant and classification of criminal participants

Figure 3 presents a typical quadrant graph according to Morselli (2010). And it was taken as the standard for our work, because many researchers found it very suitable and fundamental in similar analysis. This was presented as case A i.e., overlapping of degree centrality and betweenness centrality metrics. The graph was partitioned into four quadrants using the average of the metric values on each axis. The dotted line on the vertical axis is the average of betweenness metric values plotted on the horizontal axis while the dotted line on the horizontal axis is the average of the degree centrality metric value plotted on the vertical axis, this is further explained in section 3.2. This study used each quadrant to classify participants in organized crime into prominent, less prominent, and inconspicuous participants classes as explained in section 3.3. The Quadrant approach is believed to give a better classification than a single-metric graph. It allows the analyst to explore both the structural capacity and strategic positioning for the identification of less prominent participants.

3.2 Conception of the Structural Capacity and Strategy

A metric on the vertical axis denotes structural capacity while that of horizontal axis denotes structural strategy. Structural capacity implies feature(s) that make actors more visible to security operatives or the public. Structural-wise, a high number of direct links makes a network node become more visible to network analyst and criminal intelligence analyst. In the same way, participants in organized criminal groups (OCG) can also become more visible through the number of activities an actor might be engaged in; the influence capacity an actor has over other criminals or his ability in causing havoc based on past criminal records. It was conceptualized that conspirators with high personalities might not like to lure themselves into fierce acts as a means of identity safeguard. Since degree centrality determines the influence of an actor through its immediate neighbours in the network, there is a tendency for conspirators not to have direct neighbours significant enough to project his influence. Eigenvector centrality is conceived as an alternative for measuring influence capacity because its measurement is not restricted to immediate neighbours only. The reason for this was that the eigenvector metric was purposely developed for measuring influence in communication networks (Karthika & Bose, 2011). Influence capacity measured by eigenvector was tagged global influence capacity while that of degree centrality was tagged local influence capacity.

The structural strategy was conceived as a network-graph feature, contrary to influence capacity, this is because the latter is likely to conceal network nodes (criminal actors). It is considered as a hidden factor which can make an actor look insignificant. For example, an actor with highest betweenness centrality score can attain that with just only two links. This forces researchers to use betweenness centrality as a tool for measuring brokerage, note that brokers always occupy a strategic position. In this work, conspirators are believed to take strategic positions in criminal organizations. The proportion of brokers in OCG may depend on sparse nature and compartmentalization of the criminal structure. It cannot be denied that conspirators may have low brokerage scores due to inconspicuous links. Closeness centrality is fundamentally meant for measuring proximity; it measures the extent of an actor's distance to other nodes. An actor with the highest closeness score is often taken as a network leader because of its closeness to the centre of the structure. It is believed that conspirators are instinctive in their close relations with overt criminals (attackers), therefore it is expected that conspirators maintain a very low closeness or proximity with active criminals. Based on these considerations, we chose to use closeness centrality in place of betweenness centrality to measure strategic positioning of key player.

3.3 Classification of Identified Criminals According to Their Relevancy

The identified criminals in the data were classified according to their relevancy by inputting the paired centrality metrics, earlier grouped as cases A – D, into the simulation, then taking the mean of the centrality scores on both axes. These were plotted on the four quadrants labelled Q1 – Q4 in each of the graphs shown in figures 4 - 7. The first quadrant Q1 holds the class of the 'less prominent' participants, these are participants whose influence capacity is above average but their strategic roles are below average. The second quadrant Q2, holds the class of the 'prominent' because the participants in this quadrant have both high influence capacity and high strategic roles. It is the region where actors can become the most vulnerable to security operatives irrespective of their status or hierarchy. The third quadrant Q3, has both low influence capacity and low strategic roles. The actors that fall into this quadrant are classified as 'inconspicuous' or 'non-prominent. Finally, the fourth quadrant; Q4 has a high strategic role but low (below average) influence capacity. Q4 is the quadrant for identification of fugitive criminals (conspirators), they are classified as 'less prominent but smart criminals'. Prominent participants are highly susceptible members based on literature (Calderoni, 2010; Morselli, 2010).

High-profile criminals are assumed to emerge from quadrants Q2 and Q4. The reason behind the choice of Q2 and Q4 is that conspirators are circumventable. Circumventable participants prefer playing strategic roles (behind-the-scene activities) than overt activities. Strategic roles could be logical in promoting the prominence of conspirators than direct participations. Betweenness and closeness centrality metrics are therefore examined along with influence capacity in their effect in making conspirators become prominent. Secondly, since prominence is identified with visibility, degree and eigenvector centrality metrics are deployed to investigate which one aids prominence of conspirators more than the other. The main fact is to check if indirect relationships could make conspirators in Q3 become part of the 'less prominent' (in Q1 or Q4) or join the 'prominent' in Q2. That is, if important conspirators hiding in Q3 can be sieved out to 'less prominent' in quadrants Q1 and Q4.

4. Simulation Results and Discussion

Figure 4 depicts the plot for case A, which classified the criminals using a combination of betweenness and degree centrality. This is the general classification used in literature, but it could be seen that this classification placed almost all of the criminals as either less prominent (Q1) or inconspicuous (Q3), which means they will all evade security operatives. The very dangerous participants, i.e., the less prominent but smart criminals (Q4) were not sieved out except only one. This is also evident in Table 1, where only 18 out of 61 criminals were identified as prominent criminals (mostly in Q1) while 42 were identified as inconspicuous. From Table 2, where identified conspirators are shown, this case A was able to identified only one (1) conspirator (Q4).

Figure 5 depicts the plot for case B, which classified the criminals using a combination of closeness and degree centrality scores. This is the combination introduced in this paper, it could be seen that this sieved out more prominent criminals than any of the other cases. This is due our consideration of degree and closeness centrality measures as against the degree and betweenness centrality used in literature. This is also numerically evident in Table 1 which shows that 26 criminals were identified as prominent while 35 were identified as inconspicuous. Most importantly, this our combination sieved out more conspirators (smart criminals of Q4) than any other case, as shown in Table 2. It sieved out 8 criminals as conspirators, which are the most dangerous in criminal groups.

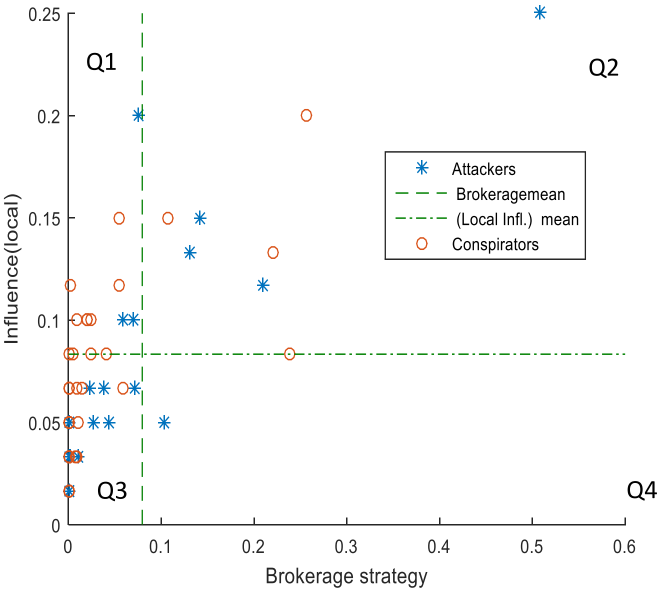

Figure 4: Brokerage position against local influence (this represents case A, i.e., the combination of degree centrality on the y-axis and the betweenness centrality on the x-axis)

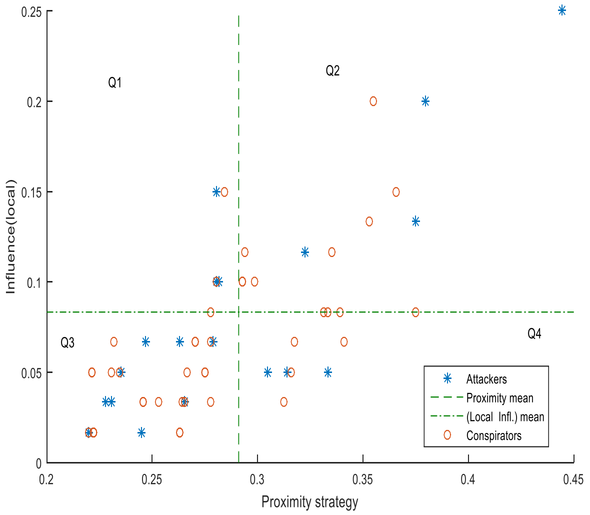

Figure 5: Proximity position against local capacity (this represents case B, i.e., the combination of degree centrality on the y-axis and the closeness centrality on the x-axis)

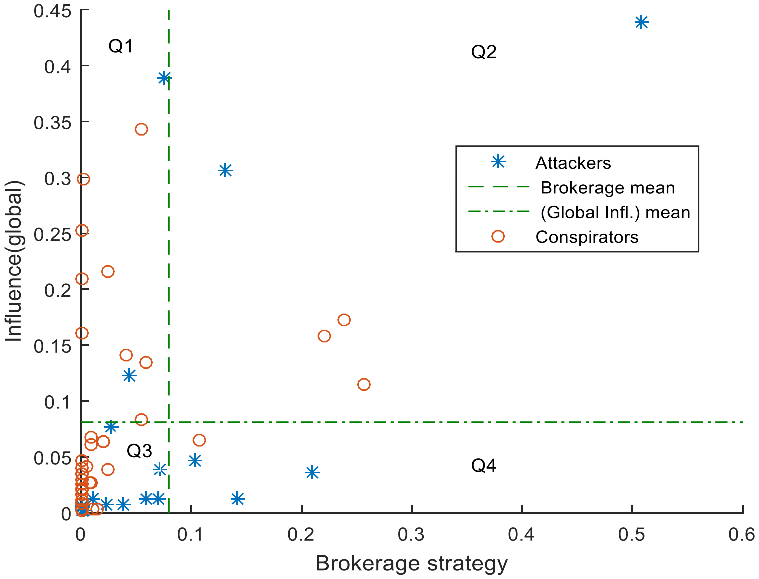

Figure 6: Brokerage position against Global capacity (this represents case C, i.e., the combination of eigenvector centrality on the y-axis and the betweeness centrality on the x-axis)

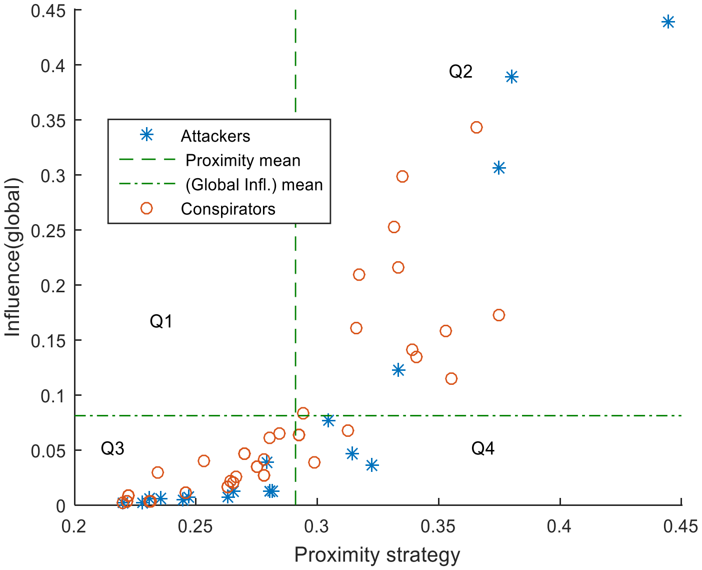

Figure 7: Proximity position against Global capacity (this represents case D, i.e., the combination of eigenvector centrality on the y-axis and the closeness centrality on the x-axis)

Figures 6 and 7 likewise shows the plot for cases C and D. These cases performed equally well but none of them classified the criminals as clearly as case B.

Table 1 presents the quantitative distribution of participants in Figures 4 through 7. Case A and C have the highest percentage of inconspicuous participants' equivalent to 68.85 percent. This percentage is higher than the benchmark percentage presented in (Morselli, 2010). This implies that betweenness renders 2 percent of participants inconspicuous to detective techniques. But closeness centrality as found in Case D reduces the number of inconspicuous participants by 2.73 percent from 66.66 to 63.93 percent, and Case B reduces by 9.29 percent from 66.66 to 57.37 percent. It can be inferred that neither local influence capacity nor global influence capacity has an impact on the number of participants that emerged as inconspicuous or prominent.

Out of 42 identified as non-prominent participants, Table 2 shows that case A has 32 and case C has 30 conspirators in column Q3. This shows that betweenness centrality as a common strategy in both cases A and C constitutes a factor for a high number of conspirators in Q3 under the local influence (degree) and global influence (eigenvector). It can be drawn that a large portion of conspirators still operate in the peripheries of the structure.

Table 1 Distribution of Prominent and Inconspicuous Participants

Participants	Prominent nodes	%Prom	Inconspicuous nodes	%Inconsp	Benchmark%
Case A	18	29.5082	42	68.8525	66.66
Case B	26	42.623	35	57.377	66.66
Case C	19	31.1475	42	68.8525	66.66
Case D	22	36.0656	39	63.9344	66.66

Benchmark is the two-third of the entire inconspicuous participants recorded in (Morselli, 2010).

Table 2 Quadrant distributions of conspirators and percentages

Conspirators	Q1	(Q1)%	Q2	(Q2)%	Q3	(Q3)%	Q4	(Q4)%	Total	Description
Case A	6	14.29	3	7.14	32	76.19	1	2.38	42	Degree/Betweenness
Case B	2	4.76	7	16.67	25	59.52	8	19.05	42	Degree/Closeness
Case C	8	19.05	3	7.14	30	71.43	1	2.38	42	Eigenvector/Betweenness
Case D	0	0	11	26.19	27	64.29	4	9.52	42	Eigenvector /Closeness

5. Conclusion

In this paper, classification of criminals using quadrant method was considered. Specifically, this method was used to sieve out conspirators who play key roles in perpetrating criminal activities but are difficult to be apprehended by security operatives. The quadrant method has been used in literature, however, only degree and betweenness centrality were considered. In this paper, in order to identify smart conspirators, who usually operate under cover, four centrality metrics were combined pair-wise in an effort to make the quadrant method more robust in detecting them. Simulation experiments were performed using the 9/11, 2001 criminal data, it was found that closeness centrality shot strategic proximity of conspirators up more than betweenness centrality, specifically 19.05% of conspirators was identified when closeness centrality was combined with degree centrality as against the 2.38% that was identified when betweenness centrality was combined with degree centrality. In addition, it was also found that indirect relationships and organizational structure did not conceal conspirators’ vulnerability. The effect was noticed in the use of degree and eigenvector centrality metrics for vulnerability capacity. However, affiliates in organized crimes as well as overt members can be classified into four subgroups with different attributes. This work is significant because it shows the possibility for criminal intelligence investigation to identify more key-players from covert networks despite data scarcity and defectiveness trailing data on OCGs.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Reference

Behzadan, V., Nourmohammadi, A., Gunes, M., & Yuksel, M. (2017). On Fighting Fire with Fire: Strategic Destabilization of Terrorist Networks. *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*, (iv), 1120–1127. https://doi.org/10.1145/3110025.3119404

Borgatti, S. P. (2006). Identifying sets of key players in a social network. *Springer*, 21–34. https://doi.org/10.1007/s10588-006-7084-x

Bright, D., Greenhill, C., Britz, T., & Ritter, A. (2017). Criminal network vulnerabilities and adaptations. *Routledge Taylor and Francis Group*, *00*(00), 1–18. https://doi.org/10.1080/17440572.2017.1377614

Bright, D., Greenhill, C., & Ritter, A. (2015). Networks within networks : using multiple link types to examine network structure and identify key actors in a drug trafficking operation. *Routledge Taylor and Francis Group*, (May), 37–41. https://doi.org/10.1080/17440572.2015.1039164

Burcher, M., & Whelan, C. (2017). Social network analysis as a tool for criminal intelligence : Understanding its potential from the perspectives of intelligence analysts. *ResearchGate*, (May), 1–18. https://doi.org/10.1007/s12117-017-9313-8

Butt, W. H., Qamar, U., & Khan, S. A. (2014). Hidden Members and Key Players Detection in Covert Networks Using Multiple Heterogeneous Layers. *Journal of Industrial and Intelligent Information*, *2*(2), 142–146. https://doi.org/10.12720/jiii.2.2.142-146

Calderoni, F. (2010). Strategic positioning in mafia networks, 198–199.

Calderoni, F. (2012). The structure of drug trafficking mafias : the ' Ndrangheta and cocaine. *Springer Science +Business Media*, 321–349. https://doi.org/10.1007/s10611-012-9387-9

Campana, P., & Varese, F. (2012). Listening to the wire : criteria and techniques for the quantitative analysis of phone intercepts. *Springer Science +Business Media*, 13–30. https://doi.org/10.1007/s12117-011-9131-3

Catanese, S., Ferrara, E., & Fiumara, G. (2013). Forensic analysis of phone call networks. *Social Network Analysis and Mining*, *3*(1), 15–33. https://doi.org/10.1007/s13278-012-0060-1

Eiselt, H. A., & Bhadury, J. (2015). The Use of Structures in Communication Networks to Track Membership in Terrorist Groups. *Journal of Terrorism Research*, *6*(1), 1–18. https://doi.org/10.15664/jtr.1073

Grassi, R., Calderoni, F., Bianchi, M., & Torriero, A. (2019). Betweenness to assess leaders in criminal networks : New evidence using the dual projection approach. *Social Networks*, *56*, 23–32. https://doi.org/10.1016/j.socnet.2018.08.001

Gunnell, D., Hillier, J., & Blakeborough, L. (2016). *Social Network Analysis of an Urban Street Gang Using Police Intelligence Data*.

Hulst, R. C. Van Der. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. *Springer*, *12*, 101–121. https://doi.org/10.1007/s12117-008-9057-6

Karthika, S., & Bose, S. (2011). A COMPARATIVE STUDY OF SOCIAL NETWORKING. *International Journal on Web Service Computing (IJWSC)*, *2*(3), 65–78.

Keller, F. B. Networks of Power : Using Social Network Analysis to understand who will rule and who is really in charge in the Chinese Communist Party (2015).

Kitsak, M., Gallos, L. K., Havlin, S., Liljeros, F., Muchnik, L., Stanley, H. E., & Makse, H. A. (2010). Identification of influential spreaders in complex networks. *Nature Physics*, *6*(11), 888–893. https://doi.org/10.1038/nphys1746

Lampe, K. Von. (2009). Human capital and social capital in criminal networks : introduction to the special issue on the 7th Blankensee Colloquium. *Springer Science+Business Media*, *12*, 93–100. https://doi.org/10.1007/s12117-009-9067-z

Leuprecht, C., Aulthouse, A., & Walther, O. (2016). The puzzling resilience of transnational organized criminal networks. *Police Practice and Research*, *17*(4). https://doi.org/10.1080/15614263.2016.1168600

Liu, Y., Tang, M., Zhou, T., & Do, Y. (2015). Core-like groups result in invalidation of identifying super-spreader by k-shell decomposition, 1–8. https://doi.org/10.1038/srep09602

Maeno, Y. (2009). Node discovery in a networked organization. *IEEE International Conference on Systems, Man, and Cybernetics*, (October), 3522–3527.

Maeno, Y., & Ohsawa, Y. (2007). Analyzing covert social network foundation behind terrorism disaster. *International Journal of Services Sciences*, *2*(x), pp.125-141. https://doi.org/10.1504/IJSSci.2009.024936

Morselli, C. (2009). Inside Criminal Networks. (F. Bovenkerk, Ed.), *Springer Science +Business Media*. Springer.

Morselli, C. (2010). Assessing Vulnerable and Strategic Positions in a Criminal Network. *Journal of Contemporary Justice*, *26*(4), 382–392. https://doi.org/10.1177/1043986210377105

Newman, M. E. J. (2002). Assortative Mixing in Networks. *The American Physical Society*, *89*, 1–4. https://doi.org/10.1103/PhysRevLett.89.208701

Ortiz-arroyo, D. (2010). Discovering Sets of Key Players in Social Networks, (November 2010), 1–20. https://doi.org/10.1007/978-1-84882-229-0

Park, O. (2018). Social Network Analysis for Law Enforcement. *International Association of Crime Analysts Iaca*, *02*, 1–19.

Qiao, T., Shan, W., & Zhou, C. (2017). How to Identify the Most Powerful Node in Complex. *Entropy*, *19*(614). https://doi.org/10.3390/e19110614

Roberts, N., & Everton, S. F. (2011). Strategies for Combating Dark Networks. *Journal of Social Structure*, *12*, 2. https://doi.org/10.1007/s10796-010-9271-z

Song, G., Zhou, X., Wang, Y., & Xie, K. (2015). Influence Maximization on Large-Scale Mobile Social Network: A Divide-and-Conquer Method. *IEEE Transactions on Parallel and Distributed Systems*, *26*(5). https://doi.org/10.1109/TPDS.2014.2320515

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, *13*(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-H

Varese, F. (2013). The Structure and the Content of Criminal Connections : The Russian Mafia in Italy. *Oxford Journals*, *29*(5), 899–909. https://doi.org/10.1093/esr/jcs067

Yang, A., Tang, Y., Wang, J., & Chen, J. (2014). Covert nodes mining in social networks based on games theory. *Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2014*, 541–545. https://doi.org/10.1109/CSCWD.2014.6846902