Hindawi Publishing Corporation
Discrete Dynamics in Nature and Society
Volume 2013, Article ID 296729, 9 pages
http://dx.doi.org/10.1155/2013/296729

Research Article

Arresting Strategy Based on Dynamic Criminal Networks Changing over Time

Junqing Yuan,[1] Jinde Cao,[1,2] and Bila Xia[3]

[1] *Department of Mathematics, Southeast University, Nanjing, Jiangsu 210096, China*
[2] *Department of Mathematics, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3] *New Star Institute of Applied Technology, No. 451 Huangshan Road, Hefei, Anhui 230031, China*

Correspondence should be addressed to Jinde Cao; jdcao@seu.edu.cn

Received 23 September 2012; Accepted 13 January 2013

Academic Editor: Xiaohui Liu

We investigate a sequence of dynamic criminal networks on a time series based on the dynamic network analysis (DNA). According to the change of networks' structure, networks' variation trend is analyzed to forecast its future structure. Finally, an optimal arresting time and priority list are designed based on our analysis. Better results can be expected than that based on social network analysis (SNA).

1. Introduction

Since September 11 attacks, focus of criminal analysis has been shifted to find terrorist networks, and a number of results have been obtained [1, 2]. Although they faced many challenges like the incompleteness, incorrectness, and inconsistency of information, they made use of the data mining and did subgroup detection to discover information. Later, they developed some visualization tools [3] to help observe criminal networks' structure. All of these must be owed to the development and maturity of SNA [4–6]. SNA was born in the 1930s, and Moreno did much foundational work for it. After that, SNA developed fast especially in the 1960s–1970s. Various metrics were defined, including centrality, clustering coefficient, and density [7–10]. However, most work was still limited on static criminal network analysis. On the other hand, a new study shows that DNA is on its way [11, 12]. DNA is an extension and evolution of SNA. It is a study combined with multiagent or multimode, full of uncertainty. Meanwhile, it introduces the domain of time into it, which makes it much more complex than SNA. In fact, our research on DNA is just staying in the beginning, and many problems are waiting to be done. For example, one should predict the traits of networks precisely and develop more techniques to visualize the outline of the whole sequence of dynamic networks. To sum up, it should be studied further.

Since the research to find the suspects and predict the crime time is still based on analyzing frequency and content of communications between suspects, which can be easily concealed and disguised by real criminals, we start from another direction, by observing a sequence of criminal networks of different time and making use of hierarch clustering to analyze the structure changes of criminal networks.

Suppose that we have got a database of message traffic records of all the criminal suspects. Of course, the time that the message is sent will be marked. Furthermore, we suppose that semantic network analysis has been finished and all the messages about crime and suspects have been extracted from the original database. So we can skip preparation part and directly focus our attention on researching the structure of criminal networks.

As our first contribution, we introduce DNA to construct a sequence of criminal networks. For the second contribution, we modify the definition of centrality and partition method based on hierarchy clustering to make it serve our model better. As our third contribution, we suggest a method, time series analysis. By this way, we can predict the possible crime time of every suspects. Finally, through analyzing the structural changes of networks, we propose four different processes to help determine the best arresting time; meanwhile, we design an arresting priority list based on the degree of importance of the suspects.

2. Establishing Dynamic Criminal Networks

Denote the time interval by Δt and divide the database of E-mail traffic into different parts according to their sending time. We regard the sending time of the earliest E-mail as the initial time; all the E-mails with sending time from 0 to Δt will be used to construct the first dynamic criminal networks $N(0)$, followed by next networks of $N(\Delta t), N(2\Delta t), N(3\Delta t)$, and so on. The network $N(i\Delta t)$ is constructed by the data between time $i \times \Delta t$ and $(i + 1) \times \Delta t$, which is unrelated to the data of other time.

Now, we get a sequence of criminal networks. For each network $N(i\Delta t)$, the nodes of the network represent the criminals who send messages during the time between $i \times \Delta t$ and $(i + 1) \times \Delta t$, and the edges represent the exchange between i and j. The weight of the edge is the times of message exchanges between i and j. These networks are all weighted undirected graphs.

In order to describe the network $N(i\Delta t)$, we first build up a relation distance matrix $M_d(i\Delta t)$ and relation strength matrix $M_r(i\Delta t)$.

Here are some notations that we will use as follows:

x: the index of member nodes;

a_{ix}: relation strength. It represents the weight on the link between nodes i and x;

d_{ix}: relation distance. It is defined as the reciprocal of a_{ix}

$$d_{ix} = \begin{cases} \dfrac{1}{a_{ix}}, & a_{ix} \neq 0 \\ \infty, & a_{ix} = 0. \end{cases} \tag{1}$$

n: the total number of nodes;

l_{ix}: the length of the shortest path between nodes i and x. The shortest path is calculated based on the Floyd algorithm.

Then, we get the relation distance matrix $M_d(i\Delta t)$:

$$\begin{bmatrix} l_{11} & \cdots & l_{1n} \\ \vdots & \ddots & \vdots \\ l_{n1} & \cdots & l_{nn} \end{bmatrix} \tag{2}$$

and relation strength matrix $M_r(i\Delta t)$:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}. \tag{3}$$

These two matrixes contain nearly all the information of the messages traffic of time between $i \times \Delta t$ and $(i + 1) \times \Delta t$, which is our basis of the following analysis and forecast.

3. Designing Modified Centrality Standard

According to Freeman's research, there are three popular centrality measures—degree centrality ($C_d(x)$), betweenness centrality ($C_b(x)$), and closeness centrality ($C_c(x)$). They are helpful in analyzing the criminal network. These three measures are used to measure the relational strength of a network. What is more, they can be used to identify key members who play important roles in a network. But it omits the frequency of transmitting messages, which is crucial to reflect the relation strength between different nodes, so we modify the above definitions and give a new definition of centrality measures as follows.

Degree centrality is defined as follows:

$$C'_d(x) = \sum_{i=1}^{n} a_{ix}, \tag{4}$$

where n is the total number of nodes in a network and a_{ix} has been defined in the previous section, which denotes a variable indicating the weighted number of messages between nodes x and i (an edge from node x to node i or from node i to node x can either be counted as a link).

Betweenness centrality is defined as follows:

$$C'_b(x) = \sum_{x}^{n} \sum_{j}^{n} g_{ij}(x), \tag{5}$$

where $g_{ij}(x)$ equals 1 if the shortest path from the node i to the node j passes through the node x; otherwise, $g_{ij}(x)$ is 0.

Closeness centrality is defined as follows:

$$C'_c(x) = \sum_{i=1}^{n} l_{ix}, \tag{6}$$

where l_{ix} is the length of the shortest path connecting nodes i and x. The shortest path is calculated based on the Floyd algorithm.

The centralities above describe different characters of nodes in a network.

(i) Degree centrality shows the number of nodes' connections, which also reflects connectivity of nodes in a network. Nodes with more connections can be viewed as more important like a leader [13] in a network.

(ii) Betweenness centrality shows the number of shortest paths passing by certain node. It also reveals the dependency of a node from other nodes. Obviously, if a node is dependent on other nodes quite much, the node must be very important for the smooth communication, like a gatekeeper [13].

(iii) Closeness centrality actually measures how far away one node is from other nodes. Apparently, small closeness value of a node reflects its high importance.

4. Clustering Analysis

Given a criminal network $N(i\Delta t)$, for the purpose of exploring the organization and structure of criminals, it is necessary to analyze its clustering or partition. And in the later part, we will find that the change of networks' structure will reveal much more information than expected. Now, the most

popular method includes hierarchy clustering [14, 15] and blockmodeling. However, always some approaches need us to determine the number of the clusters beforehand, others directly merge different clusters into one whole cluster with strict structure. Inversely, the criminal activities in the real world have become more and more complex and huge, so it is nearly impossible for few leaders to govern the whole organization; thus, emergence of criminal subnetworks is inevitable. Besides, the structure, partition, and even number of these subclusters are unknown before investigation. In this way, effectiveness of hierarchy clustering and blockmodeling may fail.

Here we design an optimal function to avoid the above problems as the following:

$$\operatorname{Max} E\left(N\left(i\Delta t\right), m, P\left(m\right)\right) = \frac{\prod_{i=1}^{m}\left(\alpha C_i\right)}{\prod_{i=1}^{n} C_d'\left(i\right)}. \tag{7}$$

Here, α is an experimental parameter, which varies from 0 to ∞ and determines the average size of subnetworks. The bigger the value of α is, the more of sub-networks will generate, but the average size of sub-networks will be smaller. And the value of α cannot be determined theoretically; it is the result of fitting according to actual cases. m represents the number of subclusters. $P(m)$ represents all the possible partitions of m clusters. C_i represents the ith subnetwork's sum of inner edges' weight after the m and $P(m)$ are determined.

This optimal function is based on the density of each subnetwork. If the partition $(m, P(m))$ is determined, then the density is defined as below:

$$D_i = \frac{\alpha C_i}{\prod_{i=1}^{k(i)} C_d'\left(i\right)}, \tag{8}$$

$K(i)$ represents the number of nodes of the subnetwork.

From the definition of density, we can find that density increases when the ratio of the inner interaction of subnetwork dominates the whole interaction of the members of the subnetworks, which reveals the information that these members are intensively connected. And we multiply all the subnetworks' densities to get the optimal function:

$$E\left(N\left(i\Delta t\right), m, P\left(m\right)\right) = \frac{\prod_{i=1}^{m}\left(\alpha C_i\right)}{\prod_{i=1}^{n} C_d'\left(i\right)} = \prod_{i=1}^{m} D_i. \tag{9}$$

It reflects the overall tight degree of all the subnetworks. The bigger the value of the optimal function $E(N(i\Delta t), m, P(m))$ is, the more intensive each subnetwork's inner structure is, and the maxima of the optimal function determines the best clustering method of the network $N(i\Delta t)$.

Below is the pseudocode of an algorithm which is designed to find the optimal value of $E(N(i\Delta t), m, P(m))$ and the best partition $P(m)$ as follows as:

input $N(t)$
set $E = \infty$, $P = \emptyset$
for i from 1 to n
do the traversal of all possible i partitions
find $\max E(N(t), P(i))$ *and* $P(i)$
if $E(N(t), P(i)) < E \quad E \leftarrow E(N(t), P(i))$ $P \leftarrow P(i)$
end if
end for

Remark 1. To find the maxima value of the optimal function, we must calculate the values of all possible partitions, which needs $O(2^n)$-space. As the p-cliques do the similar way to how our optimal function runs, we can use the method of p-cliques first as a filtration to choose adequate candidates of possible partitions. After that, we just need to verify which candidate is best by calculating their optimal functions, which will reduce the calculated scale drastically.

Remark 2. This clustering method is based on the designed optimal function; it can determine actual number and structure of subnetworks beforehand perfectly in theory. And the precondition is that α can be gotten precisely through fitting previous known criminal networks. From this way, it is an empirical function.

5. Analyzing Changes of Networks and Forecasting Future Structure

As usual, the communications between two people are rarely affected by others, and we regard the arbitrary edge's weight as being independent on other edges. So, we extract all edges' weights, respectively, from the sequence of networks and compose them of some new series:

$$W_{ij}\left(0\right), W_{ij}\left(1\Delta t\right), W_{ij}\left(2\Delta t\right), W_{ij}\left(3\Delta t\right), W_{ij}\left(4\Delta t\right), \ldots \quad 1 \ll i \ll n,\ i \ll j \ll n. \tag{10}$$

$W_{ij}(k\Delta t)$ represents the times of communication between i and j at time from $k\Delta t$ to $(k+1)\Delta t$. It also equals the a_{ix} in networks $N(k\Delta t)$.

We regard communication as an event, and $W_{ij}(k\Delta t)$ is the sum of times the events occurring in a specific time. So, every sequence composes of a time series, and we suggest the methodology in time series analysis [16] to forecast the value $W_{ij}(k\Delta t)$ of the future.

Beforehand, as different events adjust to different methods, we categorize the criminal event into two kinds.

(1) Crimes which is so serious that we must prevent them from happening in advance: terrorist attacks like 9/11, premeditated kidnaps and homicides, and so forth.

(2) Crimes which have less direct damage and can be monitored for a long term in order to obtain crucial evidence or destroy and arrest the criminal gangs entirely: drag trafficking organization, a group of traitors who steal corporation's accounts and cash, and so forth.

For the first case, it usually goes through a relatively short interval of time from the formation of criminal motive to

implementation; therefore, it lacks obvious regularity and shows a drastic trend from preparation to operation. So, we choose the ARIMA model to predict the communication behavior of every two people in the near future.

As to the second case, according to He's investigation [17], the long-term crimes have a certain degree of periodicity and meet the stationarity. We choose the ARMA model to predict long-term crime law.

This part is not the emphasis of what we discuss, and we just give the brief steps of predicting method [18].

(1) *Analyzing stationarity and operating white-noise sequence*.

(2) *Computing the values of ACF and PCF of the given data*.

(3) *Identification of ARMA model or ARIMA model*.

(4) *Estimating the unknown parameters in the model*.

(5) *Making forecast and examining the effectiveness. If it fails, choose other modes*.

(6) *Model optimization*.

(7) *Utilizing the model to forecast the future trend*.

Now, we can get the expected networks $N(T)$ at any future time permitted by conditions, so do the relation strength matrix, modified centrality, and clustering at time T. Synthesizing with the above series of networks constructed by known data, we get a new series of criminal networks:

$$\{N(0), N(1\Delta t), N(2\Delta t), N(3\Delta t), \ldots, N(n\Delta t), N((n+1)\Delta t), N((n+2)\Delta t), \ldots, N(m\Delta t)\}. \quad (11)$$

When $n \ll i \ll m$, the network of $N(i\Delta t)$ is constructed according to prediction.

Similar series of relation strength matrixes, each edge's modified centralities, and clustering networks can be gotten in the similar way.

We call these series the *expected sequence*.

6. Designing Arresting Strategy

Although criminal gangs will avoid varying their frequency of communication dramatically to avoid the sight of police, we can still determine the possible committing time of crime and the key guys according to the changes of communication clustering structure and modified centrality.

We simulate the criminals' communication process and visualize the known and predicted clustering results of the networks. By experiments, the changing trends of some structure and criminal members deserve our attention.

6.1. Merging of Two or More Subnetworks. First of all, we define that if the subnetwork of a network $N(i\Delta t)$ retains more than 50% nodes of arbitrary subnetwork of the previous network $N((i-1)\Delta t)$, then we say that the two subnetworks represent the same subgangs.

As shown in Figure 1, several subnetworks merge into one bigger subnetwork, which contains most nodes of these original subnetworks; we call this *integration process*. According to simulation, once this process happens, usually a new criminal plan will be implemented in the short term, so the best arresting time will be right before the structure of the new subnetwork stabilizes when all the members are involved and ready.

In this way, we can prevent the crimes from happening, as well, more members involved can be arrested, and more raw evidence can be obtained.

Inversely, when one big subnetwork break up into several smaller subnetworks, we call this *division process*. It usually means that one crime has just been implemented and members begin evacuating and hiding themselves. Considering this circumstance, we must catch them immediately after we find this process. The later we operate, the fewer criminals we can arrest and the less evidence we can get.

6.2. Generation of New Subnetworks. As shown in Figure 2, sometimes one derivation of one subnetwork does not come along with the disappearances of original subnetworks. It only occupies a small part of nodes of other subnetworks. We call it the *derivation process*. For the same reason, once this process happens, a new group of criminals begin to gather and plan a new crime, so we must prevent them before the new subnetwork is finally formed.

It also has its reverse process that is called *extinction process*: one subnetworks disappears with no emergence of new subnetworks. We cope it with the same way of division process.

Remark 3. Structure, differing from the microscopic behavior like several times of communications between limited individuals, is a macroscopic behavior of the whole criminal networks. So structure's change exposes more deeply the essence of the organized criminal behavior, which is beyond the control of criminals themselves. As once the structure is disguised, the following criminal networks' behavior will be distorted inevitably. It is easily to understand. Every member of the criminal gangs, even the leaders, only contacts limited members and information, which, in one way, ensures security by a certain degree of isolation; in another, is caused by distrust between different subgangs. So no one in the gangs can know and determine the whole criminal network. But we can detect and research the whole network by monitoring their communications.

Remark 4. Here, we just list and analyze four simplest possible processes. Other more complex processes like derivation of two or three bigger subnetworks and division into three-tier subnetworks or four-tier subnetworks, although can be realized in theorem, are too complicated for actual criminal activities. So, we omit the further discussion. Certainly, other possible processes are worthy to find in the future study.

6.3. Determination of Core Members. In the process of capturing, usually it is hard to catch all the members, as

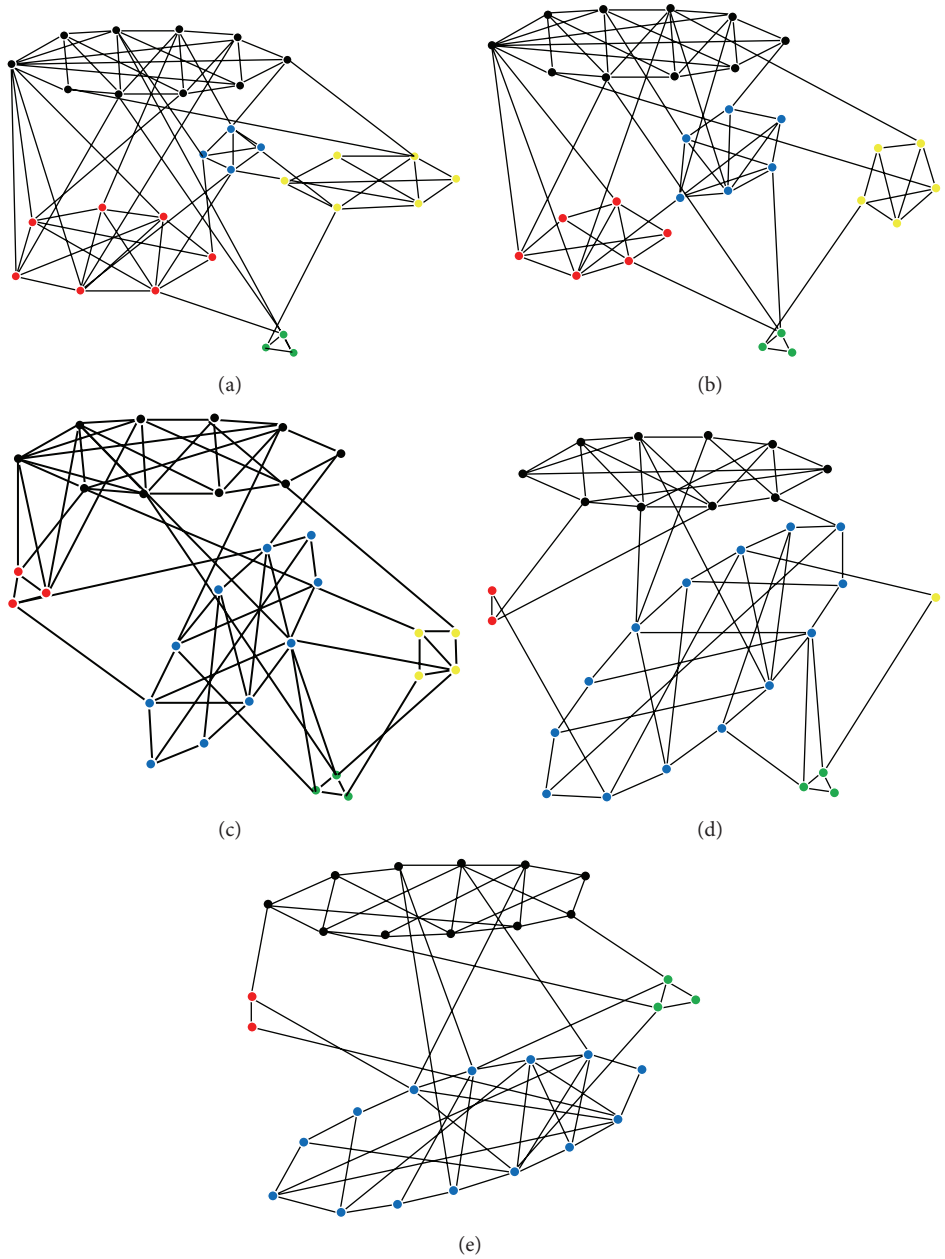


Figure 1: It is a visualization of change of networks' structure in a predicted sequence from $i\Delta t$ to $(i+4)\Delta t$, which shows a simple integration process. Different partitions are distinguished by different colors of nodes.

each capturing will invite others' alertness. Therefore, it is an urgent work to find the core members and catch them firstly. Here, we make use of the expected sequences of modified centrality's of every node who is involved in the newly emerging subnetwork during the integration process or derivation process. Through investigating their changing trend, we are hopefully to find those key guys.

(a) If some nodes whose degree centrality shows an increasing trend and reaches the peak among others' in the expected sequences, then according to the above conclusion, they are more possible to be the leaders of this subnetworks. We should catch them firstly.

(b) If some nodes whose betweenness centrality shows an increasing trend and reaches the peak among others' in the expected sequences, then these guys are likely to be the gatekeepers, who make sure the smooth of communication. Catching them will invite others' alertness immediately. So, we should watch them closely and arrest them lastly.

(c) As to other members, we use the method of TOPSIS [19] to determine their importance.

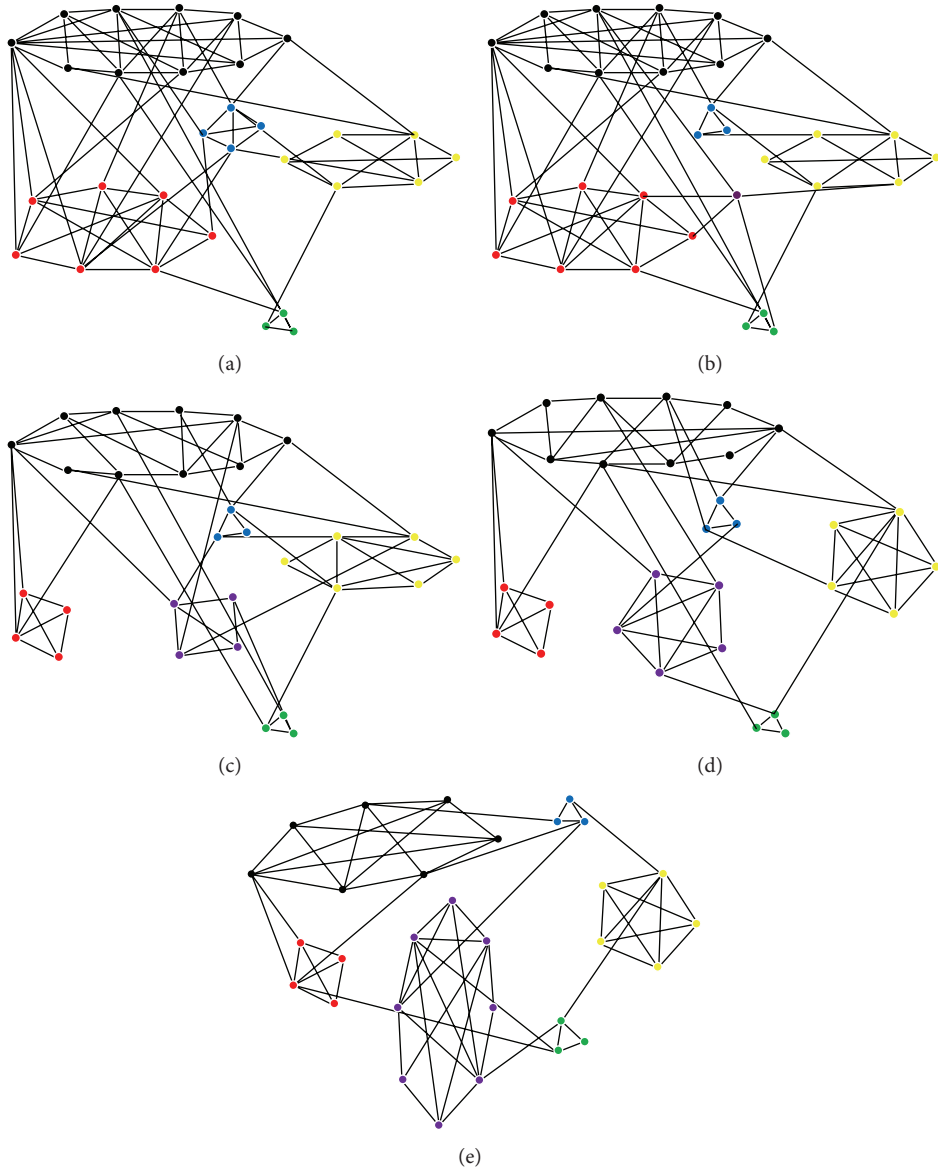


FIGURE 2: It is a visualization of change of networks' structure in a predicted sequence from $i\Delta t$ to $(i+4)\Delta t$, which shows a simple derivation process. Different partitions are distinguished by different colors of nodes.

Beforehand, we define some new notations.

A_x: the vector contains the three centrality measures.

A^C: the ideal value of A_x represents the one that is sure to be conspirator.

A^N: the ideal value of A_x represents the one is sure to be nonconspirator.

$D_C(x)$: the euclid distance defined represents the relevancy between a suspicious person and the ideal conspiratorial value A^C.

$D_N(x)$: the Euclid distance defined represents the relevancy between a suspicious person and the ideal nonconspiratorial value A^N.

According to the above analysis, we define a vector of trituple which contains three measures of the form as follows:

$$A_x = \left(\frac{C'_d(x)}{\max_x C'_d(x)}, \frac{C'_b(x)}{\max_x C'_b(x)}, \frac{C'_c(x)}{\max_x C'_c(x)} \right). \quad (12)$$

For the convenience of description, A_x is called *measure vector*. It can also be represented in another form as below:

$$A_x = (A_{x1}, A_{x2}, A_{x3}), \quad (13)$$

where A_{xi} $(i = 1, 2, 3)$ stands for element i in the vector A_x. Three elements are all divided by the maximum value of the values from data of all people we are concerned about. The aim of the division is to make sure that $0 \leq A_{xi} \leq 1$ $(i = 1, 2, 3)$. According to the definition of three centralities, it

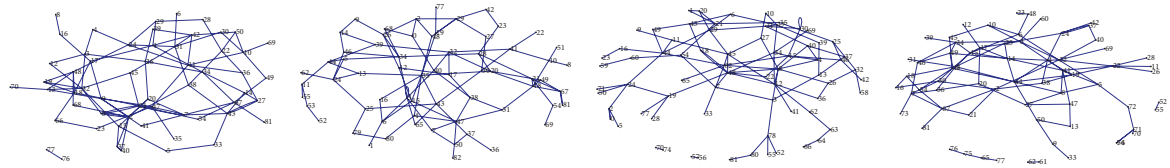


Figure 3

is obvious that A_x will get its optimal value when degree (A_{x1}) and betweenness (A_{x2}) get to their largest value 1, while closeness (A_{x3}) gets to its smallest value 0.

Therefore, the ideal model of a person who is most crucial among the criminal gangs will have his own measure vector A_x as $(1, 1, 0)$, while the ideal model of a person who plays marginal role will have his own measure vector A_x as $(0, 0, 1)$. These two ideal vectors will be defined as A^C and A^N:

$$A^C = \left(A_1^C, A_2^C, A_3^C\right) = (1, 1, 0),$$
$$A^N = \left(A_1^N, A_2^N, A_3^N\right) = (0, 0, 1). \tag{14}$$

What we need to do is to calculate the A_x value of every node. The measure vector A_x can be used to calculate the "distance" among the nodes. Based on the idea of ranking method from TOPSIS algorithm, we call the "distance" as *suspect distance*, which is defined as below:

$$D_C(x) = \sqrt{\left(A_{x1} - A_1^C\right)^2 + \left(A_{x2} - A_2^C\right)^2 + \left(A_{x3} - A_3^C\right)^2}. \tag{15}$$

This distance is the key to determine the priority list of who are more crucial. A further distance apparently indicates a lower possibility of being a key member. On the other side, if the $D_c(x)$ of the arbitrary node x is quite close to 0, then the one represented by the node x must be quite possible a leader or somebody.

Similarly, we can define the Euclid distance of A_x from the node x to the ideal A^N as $D_N(x)$, which is called *innocence distance*. The definition is

$$D_N(x) = \sqrt{\left(A_{x1} - A_1^N\right)^2 + \left(A_{x2} - A_2^N\right)^2 + \left(A_{x3} - A_3^N\right)^2}. \tag{16}$$

The suspicious members in the subnetworks will be arranged into an initial priority list. The order of the list is arranged according to the value of $D_C(x)$. Node with smaller $D_C(x)$ will be ranked higher in the priority list since $D_C(x)$ is the distance from the node to an ideal "conspirator" node. It is also worth mentioning that node with smaller $D_C(x)$ value is also with larger $D_N(x)$ value, and this demonstrates the correction of our method. Finally, we can determine to catch which one comes first according to this priority list.

7. An Illustrative Example

Here, we use the data from ICM 2012 problems [20]. First, we use the ARMA model offered by program package of software R to forecast the crime networks in the future (see Figure 3).

The first three crime networks are drawn by the given data; the forth one is the result of ARMA model. The indexes of nodes from 1 to 82 represent 82 potential crimes, and the edges between two nodes indicate the two people have been that communicating.

Then, we use the method from clustering analysis and software Pajek to give the result of partition of known crime networks at Δt, $2 * \Delta t$, and $3 * \Delta t$.

As we have got the partition of known crime networks and the prediction of future crime networks, now, we can combine them with time series analysis and clustering analysis to forecast the partition of crime networks at $4 * \Delta t$.

Similarly, we give the 3D picture of Figure 5.

Observing Figures 4 and 6, we can find that the partition of green part has a growing trend with a decreasing acceleration. In Figure 6, the partition of green part has become constant gradually.

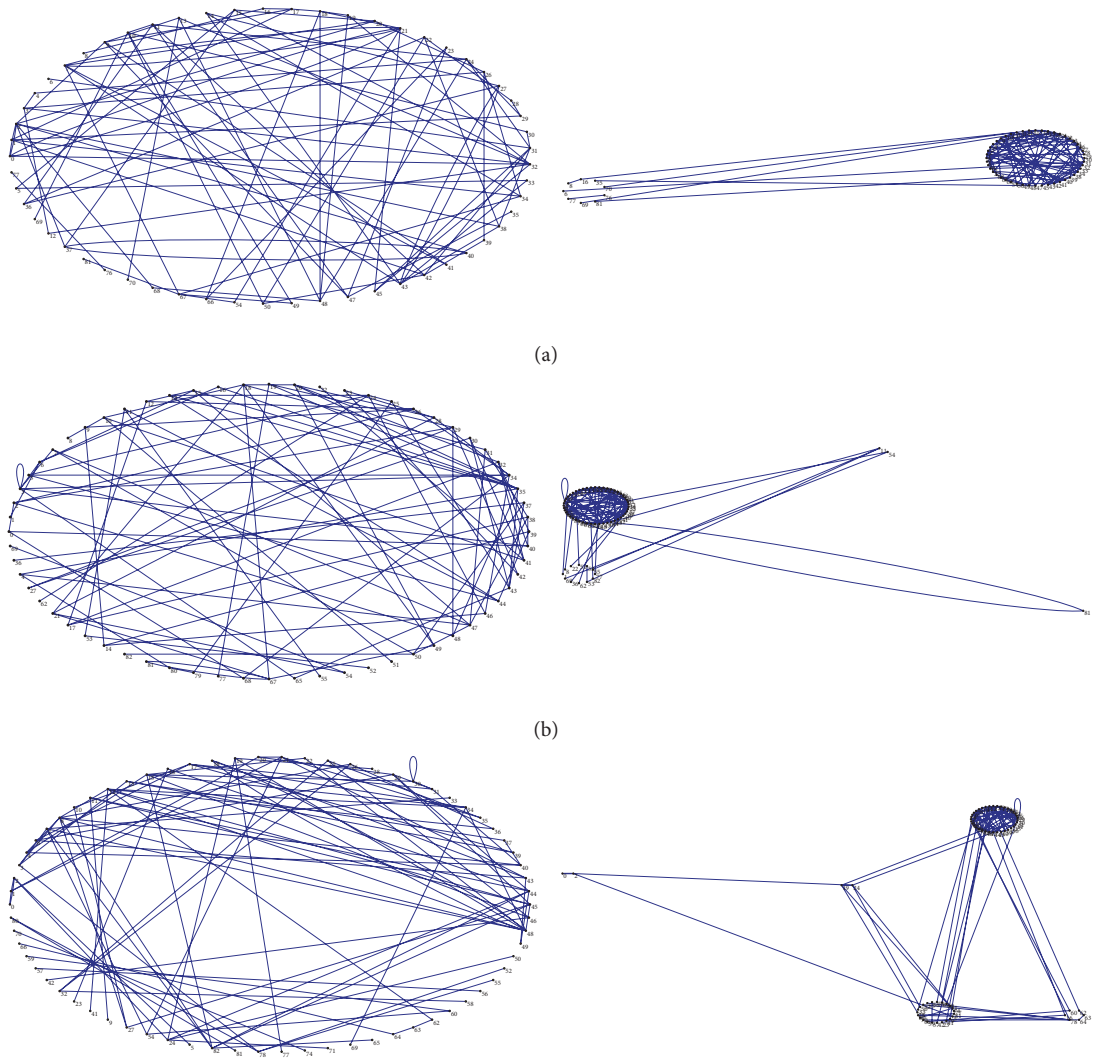
According to the implication from Figures 4 and 6, there is a high possibility that the criminals represented by green nodes were planning a new crime and would come to maturity at $4 * \Delta t$, which merits the high attention of the police.

8. Conclusion

To choose different perspectives to analyze problems, it will usually obtain some new feelings. In order to close the essence of the criminal network, we abandon the common SNA and frequency analysis or density analysis in DNA, and instead, we observe the overall structure's change of networks. Although it is hard to analyze quantitatively, we can visualize this process and observe it directly. In this way, we exemplify our superiority to touch overall networks' image, which is hard for criminals to disguise.

Acknowledgments

This work was jointly supported by the National Natural Science Foundation of China under Grant nos. 61272530 and



(a)

(b)

(c)

Figure 4: Left column is the exact result of partition of crime networks at Δt, $2 * \Delta t$, and $3 * \Delta t$; right column shows the visualization results of partition in 3D space. The nodes with the same color mean that they belong to the same partition.

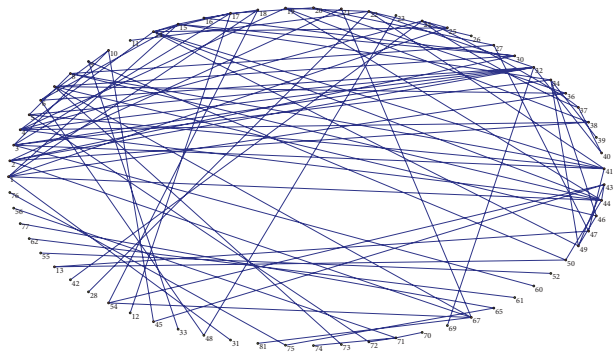


Figure 5: The future partition of crime networks at $4 * \Delta t$.

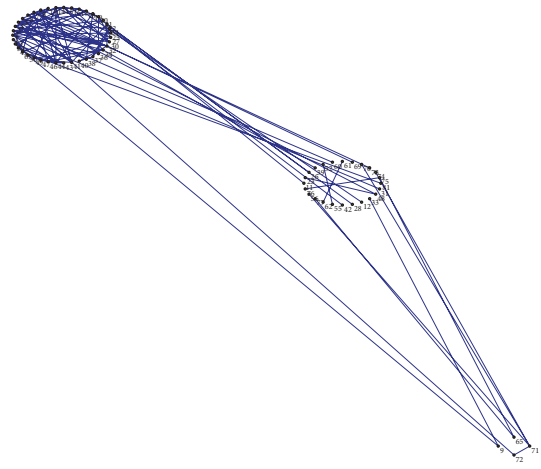


Figure 6: 3D picture of last table.

11072059 and by the Natural Science Foundation of Jiangsu Province of China under Grant no. BK2012741.

References

[1] X. Jennifer and H. Chen, "CRIMINAL network analysis and visualization," *Communications of the ACM*, vol. 48, no. 6, pp. 100–107, 2005.

[2] J. Xu and H. Chen, "Untangling criminal networks: a case study," in *Intelligence and Security Informatics*, vol. 2665 of *Lecture Notes in Computer Science*, pp. 232–248, 2003.

[3] W. D. Nooy, A. Mrvar, and V. Batagelj, *Exploratory Social Network Analysis With Pajek*, Cambridge University Press, 2005.

[4] P. Carlos, *Social Network Analysis in Telecommunication*, John Wiley & Sons, 2011.

[5] A. D'Andrea, F. Ferri, and P. Grifoni, *An Overview of Methods for Virtual Social Network Analysis*, Springer, 2009.

[6] L. Freeman, *The Development of Social Network Analysis*, Empirical Press, 2006.

[7] D. Hansen, B. Shneiderman, and M. A. Smith, *Analyzing Social Media Networks With NodeXL*, Morgan Kaufmann, 2010.

[8] L. Bing, *Web Data Mining: Exploring Hyperlinks, Contents and Usage Data*, Springer, 2011.

[9] H. Robert and R. Mark, "Concepts and measure for basic network analysis," in *The Sage Handbook of Social Network Analysis*, pp. 364–367, 2011.

[10] T. Maksim and K. Alexander, *Social Network Analysis for Startups: Finding Connections on the Social Web*, O'Reilly, 2011.

[11] K. M. Carley, "Dynamic network analysis," in *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*, pp. 135–145, 2002.

[12] K. M. Carley, "Smart agents and organizations of the future," in *The Handbook of New Media*, pp. 206–220, 2002.

[13] J. J. Xu and H. Chen, "CrimeNet explorer: a framework for criminal network knowledge discovery," *ACM Transactions on Information Systems*, vol. 23, no. 2, pp. 201–226, 2005.

[14] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan, "A cluster-based approach for routing in dynamic networks," *ACM SIGCOMM Computer Communication Review*, vol. 27, no. 2, pp. 49–64, 1997.

[15] A. K. Jain, M. N. Murty, and P. J. Flynn, "Data clustering: a review," *ACM Computing Surveys*, vol. 31, no. 3, pp. 316–323, 1999.

[16] G. Janacek, "Time series analysis: forecasting and control," *Journal of Time Series Analysis*, vol. 31, no. 4, p. 303, 2010.

[17] P. He, "Research on the theory of social crime statistics and time series survey," *Journal of Liaoning Police Academy*, vol. 3, no. 2, pp. 1–5, 2005 (Chinese).

[18] Y. Tang and Q. Ni, "Applications of ARMA model in prediction problems," *Journal of Jiaxing University*, vol. 18, supplement 1, pp. 183–187, 2006 (Chinese).

[19] H. S. Shih, H. J. Shyur, and E. S. Lee, "An extension of TOPSIS for group decision making," *Mathematical and Computer Modelling*, vol. 45, no. 7-8, pp. 801–813, 2007.

[20] http://www.comap.com/undergraduate/contests/mcm/contests/2012/problems/.