Neurocomputing 140 (2014) 121–127

Contents lists available at ScienceDirect

Neurocomputing

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

Solution to gang crime based on Graph Theory and Analytical Hierarchy Process

Yulong Gao, Yuanqing Xia*, Suichao Wu, Jianan Qiao

School of Automation, Beijing Institute of Technology, Beijing 100081, PR China

ARTICLE INFO

Article history:
Received 12 June 2013
Received in revised form
20 October 2013
Accepted 16 February 2014
Communicated by Lixian Zhang
Available online 28 April 2014

Keywords:
Gang crime
Network
Graph Theory
AHP
Semantic analysis

ABSTRACT

This paper considers the solution to gang crime combined Analytical Hierarchy Process with Graph Theory. The main purpose is to identify the conspirators and make a priority list based on the given message traffic in a certain crime case. To identify one person, we firstly quantify the topics through Analytic Hierarchy Process, then establish the network model based on Graph Theory and finally conclude the relative relevance from this person to the known conspirators and non-conspirators. The flexibility of the model is illustrated and the results show that the method is effective.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

The knowledge explosion of science encourages the invention of new technologies and contributes to the increase of economy and enhancement of human lives. However, along with these improvements, the crime also presents the high-tech and gang characteristics [12]. For example, there are always some lawless persons capturing loopholes and thus causing some troublesome problems like internet intrusion and internet fraud [1,22], which are detrimental to citizen's life and possessions. Compared to the original types of criminal, the high-tech and gang characteristics exaggerate both the detriments of these crimes and the complicity to solve them. Although it is easy to capture some shadow conspiracy messages, it is a complex and time-consuming job to detect most conspirators from the large message traffic.

In recent years, many algorithms and methodologies have been developed in allusion to this kind of crime problem. Mohammad A. Tayebi and Uwe Glässer applied mathematical models of crime data and criminal activity as underlying semantic foundation to identify organized crime structures in Co-offending Networks in [18]. In the work of [10], N. Léchevin, C.A. Rabbath and P. Maupin proposed a stability monitoring system of an Asset-Communications Network exposed to malicious attacks. Christopher C. Yang and Tobun D. Ng established a crawler to extract specific topics for the Weblog to analyze and visualize terrorism and crime related Weblog Social Network in [24]. Furthermore, Network has been studied in different areas. Many scholars pay more attention to Networked Control Systems (NCSs) and [30] has concluded the methodologies for NCSs with network-induced constraints. Zhang and Shi [31] have constructed a parameterized reduced-model for a class of discrete-time switched linear parameter varying systems and model predictive control of networked control systems (NCSs) with uncertain time delay and data packets disorder has been proposed to deal with the bounded and arbitrary delays in [27]. In addition, among the researches related to the criminal topic, semantic analysis is commonly applied. V. Loia and the fellow authors integrate Computational Intelligence techniques and Semantic Web methodologies to investigate a computer crime in [14]. Semantic methodology has also been applied in extracting crime information from text in [21] and website in [25]. Besides, Semantic analysis has also been combined with other theories to process crime problems, see for example [23]. Semantic analysis has been widely used in many other fields like linguistic [5,8,15], Image Processing [11,17] and website service [9]. Also, Semantic analysis has been combined with other methodologies like Genetic Algorithm [16,32], Statistical Relations [13] and Graph Theory [4,20] to tackle problems in other fields besides criminology. However, the combination of semantic analysis, Graph Theory and Analytic Hierarchy Process (AHP) [2,3,6,26] is

* Corresponding author.
E-mail addresses: dfgaoyulong@sina.com (Y. Gao), xia_yuanqing@bit.edu.cn (Y. Xia), wu_suichao@126.com (S. Wu), qjn83@163.com (J. Qiao).

http://dx.doi.org/10.1016/j.neucom.2014.02.041
0925-2312/© 2014 Elsevier B.V. All rights reserved.

initially adopted in this paper for solving the gang crime problem of 2012 The Interdisciplinary Contest in Modeling (ICM).

The Analytic Hierarchy Process is a structured technique for organizing and analyzing complex decisions. Based on mathematics and psychology, it was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then. It has been widely applied to decision making in various areas such as economics, finance, politics, games and sports [28]. For example, Robert L. Nydick and Ronald Paul Hill used the AHP method to structure the supplier selection process in [29]. Compared with other methods like cosine transformation and circuit equivalence, AHP is both flexible and more smart, it can decrease the subjectivity of human judgment by classifying the hierarchy structure in detail and normalization process, and the human judgment can also figure out some latent useful messages to increase the accuracy of the results. Graph Theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. In our model, the application of Graph Theory can help decrease the subjectivity caused by human judgment through meticulous mathematical calculation.

In order to find out the conspirators and make a prior list, we firstly quantify the topics through AHP and obtain their weights to measure their suspicious degree. Then, based on Graph Theory, we establish the network model and calculate the relevance between any two persons using Dijkstra Algorithm [7,19,25]. Finally, we take the sensitivity analysis and discuss the strengths and weaknesses of our model. Furthermore, we introduce keyword index and semantic analysis to establish an Artificial Intelligence System. It can give the priority list of conspirators automatically and diminish the subjectivity to enhance our model.

2. Problem formulation

The crime busting problem describes a gang crime. The conspirators and the possible suspected conspirators all work for the same company in a large office complex. As shown in Fig. 1, ICM offers a small set of messages from a group of 82 workers in the company that they believe will help them find the most likely candidates for the unidentified co-conspirators and unknown leaders. Since the message traffic is for all the office workers in the company, it is very likely that some (maybe many) of the identified communicators in the message traffic are not involved in the conspiracy. In fact, they are certain that they know some people who are not in the conspiracy. Specific information about the problem can be found in [1]. In this paper, we focus on two requirements.

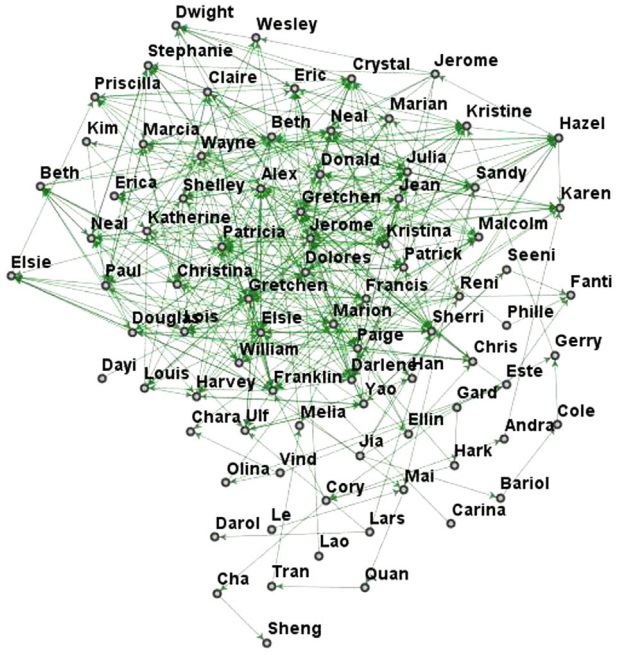

Fig. 1. The network graph.

Requirement 1: It is known that the crime busting case has 83 nodes, 400 links (some involving more than 1 topic), over 21,000 words of message traffic, 15 topics (3 have been deemed to be suspicious), 7 known conspirators, and 8 known non-conspirators. Build a model and algorithm to prioritize the 83 nodes by likelihood of being part of the conspiracy and explain the model and metrics. Jerome, Delores, and Gretchen are the senior managers of the company. It would be very helpful to know if any of them are involved in the conspiracy.

Requirement 2: How would the priority list change if new information comes to light that Topic 1 is also connected to the conspiracy and that Chris is one of the conspirators?

We specifically focus on the topics given in the attachment and model the crime busting using network analysis. Our goals are to

- identify people in the office complex who are the most likely conspirators;
- make a priority list;
- draw a discriminate line separating conspirators from non-conspirators;
- nominate the conspiracy leaders;

Before we start, some basic assumptions are needed in order to simplify the model.

- As Managers, they have more opportunities to communicate with employers;
- the conspirators' identifications remain unchanged;
- we discriminate the office personnel only by serial number instead of their names, namely, the condition that two or more people possess the same name exists.

3. Our approach

3.1. Variables

- T_k refers to the weight of the kth topic;
- D is a matrix where d_{ij} is an element of D and indicates the relevance between person i and j;
- c_i refers to the average of the sum of the shortest paths from person i to all the conspirators;
- g_i refers to the average of the sum of the shortest paths from person i to all the non-conspirators;
- r_i refers to the suspicious degree of person i.

3.2. Our model

To establish our model, we firstly quantify the topics through Analytic Hierarchy Process and obtain their weights to measure their suspicious degree. Then, based on the weights of topics and Graph Theory, we establish the network model and calculate the relevance between any two persons using Dijkstra Algorithm. To identify Person i, we conclude r_i which indicates the relative relevance from this person to the known conspirators and non-conspirators.

3.2.1. Quantify the topics

The Analytic Hierarchy Process is a structured technique for organizing and analyzing complex decisions. Based on mathematics and psychology, it was developed by Thomas L. Saaty in the 1970s and

Download English Version:

https://daneshyari.com/en/article/406674

Download Persian Version:

https://daneshyari.com/article/406674

Daneshyari.com