Chapter 6
Social Network Inspired Approach to Intelligent Monitoring of Intelligence Data

Qiang Shen
Aberstwyth University, UK

Tossapon Boongoen
Royal Thai Air Force Academy, Thailand

ABSTRACT

In the wake of recent terrorist atrocities, intelligence experts have commented that failures in detecting terrorist and criminal activities are not so much due to a lack of data, as they are due to difficulties in relating and interpreting the available intelligence. An intelligent tool for monitoring and interpreting intelligence data will provide a helpful means for intelligence analysts to consider emerging scenarios of plausible threats, thereby offering useful assistance in devising and deploying preventive measures against such possibilities. One of the major problems in need of such attention is detecting false identity that has become the common denominator of all serious crime, especially terrorism. Typical approaches to this problem rely on the similarity measure of textual and other content-based characteristics, which are usually not applicable in the case of deceptive and erroneous description. This barrier may be overcome through link information presented in communication behaviors, financial interactions and social networks. Quantitative link-based similarity measures have proven effective for identifying similar problems in the Internet and publication domains. However, these numerical methods only concentrate on link structures, and fail to achieve accurate and coherent interpretation of the information. Inspired by this observation, the chapter presents a novel qualitative similarity measure that makes use of multiple link properties to refine the underlying similarity estimation process and consequently derive semantic-rich similarity descriptors. The approach is based on order-of-magnitude reasoning. Its performance is empirically evaluated over a terrorism-related dataset, and compared against several state-of-the-art link-based algorithms and other alternative methods.

DOI: 10.4018/978-1-61350-513-7.ch006

INTRODUCTION

Most criminal and terrorist organisations form flexible networks of loosely related individuals and sub-organisations (units). These networks are often embedded within legitimate society and they evolve over time to attain their concealment. However, organised crime and terrorist activity does leave a trail of information, such as captured communications and forensic evidence, which can be collected by police and intelligence organisations. Whilst experienced intelligence analysts can suggest plausible scenarios based on such information, promptly identifying potential organisations that pose a threat, the amount of intelligence data possibly relevant may well be overwhelming for human examination. Automated hypothetical (re-) construction of the organisations and activities that may have generated the intelligence data obtained, therefore, presents an important and challenging research for crime prevention and detection.

The effectiveness of initial automated decision-support systems, such as COPLINK (Chen et al., 2003) and the Universal Situational Awareness (USA) system (Rubin and Lee, 2003), is crucially dependent upon the experience of the user/analysts as the potential threats are identified only by the analysts. This vulnerability has been addressed by systems such as those reported in (Keppens et al., 2005) and (Shen et al., 2006), which automatically generate plausible scenarios when given a limited amount of real or hypothesised evidence. These systems also provide the user with the means to analyse such scenarios and offer helpful information that may enhance efforts for crime reduction. However, the problem of identity disambiguation which is commonly encountered in intelligence data analysis (Badia and Kantardzic, 2005; Wang et al., 2006) has not been addressed thus far. In fact, a modest resolution typically used within the existing crime investigation systems is to assume that the identities of any instances (e.g., person, object, place, and organisation) involving in a reasoning process are globally unambiguous. However, this simple ignorance of possible identity aliases drastically reduces the degree of this approach's flexibility and actual utilisation within the real world. The quality of generated crime scenarios may be enhanced through the resolution of duplicated references. This additional mechanism helps to reveal an unforeseen scenario that may be overlooked otherwise (Fu et al., 2010; Fu and Shen, 2010).

In the context of terrorism and organised crimes, such a task is not straightforward as most duplications are subject to deception. Holders of a false identity intend to avoid accountability and to leave no traces for law enforcement authority. Identity fraud is intentionally committed with a view to perpetrating another crime from the most trivial to the most dreadful imaginable. Especially in the case of terrorism, it is widely utilised to provide financial and logistical support to terrorist networks that have set up and encourage criminal activities to undermine civil society. Tracking terrorist activities undoubtedly requires authentic identification of criminals and terrorists. Particularly to the September 11 terrorist attacks, tragic consequences could have been prevented to a certain extent if U.S. authorities had been able to discover the use of deceptive identity, e.g., multiple dates of birth and alias names. In such circumstance, identity verification and name variation detection systems (e.g., (Blienko et al., 2003; Torvik et al., 2004)) that rely solely on the inexact search of textual attributes are partially effective. Nevertheless, these methods will fail to disclose the unconventional truth where highly deceptive identities (e.g., 'Usama bin Laden' and 'The prince') refer to the same person.

The aforementioned dilemma may be overcome through social network analysis (SNA) (Ting et al., 2010; Wasserman and Faust, 1994) or link analysis (Getoor and Diehl, 2005), which seeks to discover knowledge based on the relationships in data about people, places, things, and events. Intuitively, despite using distinct false identities, each terrorist normally exhibits unique relations