Applying Social Network Analysis Techniques in Crawler Based Search Engine to Support Web Terrorism Mining

Amin Shahraki Moghaddam[1], Javad Hosseinkhani[2], Suriayati Chuprat [2], Anoosh Mansouri Birgani [1], and Solmaz Keikhaee[3]

Department of Computer, Zahedan Branch, Islamic Azad University,Zahedan,Iran[1]
Zahedan, Iran
Advanced Informatics School (AIS),Universiti Teknologi Malaysia (UTM)[2]
Kuala Lumpur, Malaysia
Department of Electrical, Zahedan Branch, Islamic Azad University,Zahedan,Iran[3]
Zahedan, Iran

Summary
Terrorism is a man-made phenomenon. It causes huge economic, social and environmental collisions. Criminal web data offer unidentified and precious data for Law enforcement organizations incessantly. The digital data which is used in forensics investigation contains member of information regarding the suspects' social networks. Though, there is demanding subject regarding investigating these sections of information. The terrorist association network has been used for research due to its complex of people who distributed from groups to groups and have an effectual power of their philosophy all over the world. The major goal of this research is to tackle the process of examining the criminal believes of forensic data investigation regarding prioritizes capable links and pages which wrap the reliability and consistency gap by offering a framework. This study will also argue a variety of open issues in this area.

Key words:
Web Crime Mining, Terrorist Network, Criminal Network Analysis, Social Network.

1. Introduction

Anonymous and suitable information always are provided by criminal web data for Law enforcement agencies. The evaluation of the different capacities of widespread criminal web data is very difficult all the time so it is one of the most noteworthy tasks for law administration. Crimes may be as extreme as murder and rape where advanced analytical methods are required to extract useful information from the data. Web mining comes in as a solution [1, 2].

From the Sept. 11, 2001, the fear of characteristics confirmation got new heights. Investigating identity deception attracts more interest these days with national security issues. Identity deception is an intentional falsification of identity in order to deter investigations. Conventional investigation methods run into difficulty when dealing with criminals who use deceptive or fraudulent identities, as the FBI discovered when trying to determine the true identities of the 19 hijackers involved in the attacks. Besides its use in the post - event investigation, the ability to validate identity can also be used as a tool to prevent future tragedies.

In many suspect situations, suspicions have measured the computers for instance desktops smart phones notebooks. Computers have an important knowledge and information about social networks of the suspect, they also are the main target of criminal [16].

Terrorist associations are proper to investigate deploying social network investigation, as they contain of complexes of people that span regions, groups, and economic condition, and shape about a precise ideology. Terrorist associations are dissimilar from hierarchical, state-sponsored appointments in specifications such as management and organizational arrangement. Social network investigation can supply significant data on the sole specifications of terrorist associations, varying from network recruitment issues, network development, and the dispersal of radical thoughts.

Network investigation can be deployed to appreciate the mental consequence of terrorism. One of the major impacts of terrorism is horror, which is distributed throughout network organizations such as media, the Internet, and individual associations. For instance, the quantity of ties a person has to wounded of terrorism may affect the person's awareness of the terrorism's risk.

Due to the new evolving trends of security problems, a new type of intelligence is needed which is called as Social Network Analysis (SNA).The basis of social network analysis is that individual nodes are connected by complex yet understandable relationships that form networks. These networks are said to be pervasive in nature with their own law and orders framed. But a drawback with SNA is that it cannot be considered as an appropriate data mining technique because it can discover the patterns from the known structure and not from hidden structure like a terrorist network where the nodes are embedded in a large population. Hence the knowledge discovery process to

Manuscript received August 5, 2017
Manuscript revised August 20, 2017

isolate overt cell from covert cell uses the crime data mining technique and the hidden network is analyzed using Criminal Network Analysis (CNA).

For crawling of the Web, many applications exist. One is surfing on the Internet and visiting web sites, it can help a user to notify when new information updated. Wicket applications also exist for crawlers such as the spammers or theft attackers who use the email addresses to collect personal information. However, supporting the search engines is the most common use of crawlers. Actually, the main clients of Internet bandwidth are crawlers that help search engines to gather pages and build their indexes for example, proficient universal crawlers designed for research engines such as Google, Yahoo and MSN to collect all pages regardless of the content. Other crawlers are called preferential crawlers who are attempting to download only pages of certain types or topics and they are more targeted. A suggested framework uses a special crawler for crime web mining. Special crawlers are one that go and bring the web pages based on the ranking [12, 2].

This study has principally two goals that is: classifying a variety of methods by means of CNA for investigating the covert networks and offering short information of the different kinds of investigation and units of investigation on which the network is appreciated and second goal is to tackle the process of examining the criminal believes of forensic data investigation regarding prioritizes capable links and pages which wrap the reliability gap by suggesting a framework.

The suggested framework of this research for web crime mining contains two parts. The primary part is High-level design of a crawler, the crawl the web that built on graded pages which content mining grade the downloaded pages to determine key URLs early part all over the crawl. The subsequent part is criminal networks mining. To decrease the running time of the process in ranking URLs for swarming the favorite pages, the priority algorithm is deployed.

2. Social Network Analysis

The worth of social network hypothesis against further political discipline and sociological methods is its concentration on the worth of the network configuration more willingly than the specifications of the person. Whilst social network investigation foliage's room for persons to influence their fortune, it discusses that the organization of the network and connections and ties with others in the network are more significant. The network construction of an association (in this case a terrorist association) will influence its capability to admittance novel thoughts, recruit novel people, and attain sustainability. Network investigation appears to effort since it offers a structural investigation while still leaving room for person endeavor. Briefly, network investigation constructs upon many managerial hypothesis, because networks are just an additional managerial arrangement.

Social network investigation is the recognition of the "most significant" actors in a social network. In this segment the paper investigates a diversity of metrics intended to emphasize the dissimilarities among imperative and non-imperative actors. These complete metrics try to explain and gauge the specifications of "actor location" in a social network. All these metrics are first described at the level of person actor. The metrics can then be integrated over all actors to obtain a group level metric of centralization.

Famous actors are those that are broadly concerned in associations with other actors. The centrality can be calculated in both non-directional relations and directional relations. Different from the directional relation in non-directional relation, centrality of the node does not rely on being a receiver or foundation. There are three mainly used actor-level directories that is degree centrality, closeness centrality, betweeness centrality [17].

3. Social Network Analysis and Terrorism

In this part the research illustrates the categorization of CNA approaches for terrorist networks which is shown in Figure 1.

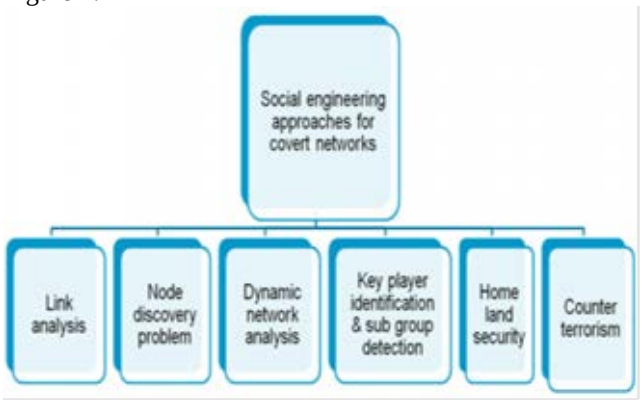

Fig. 1 Taxonomy of various criminal network analysis techniques [11]

A. Link Analysis

CNA needs the capability to incorporate information from numerous crime occurrences where the relations among crime units are known deploying link investigation [13].

Christopher C. Yang and Tobun D. Ng [18] argue the issues in investigating relations within the semantics of bloggers' messages since weblog social network does not employ page grades or indexing methods. The authors

have developed a crawler called as Dark web which does link and content investigation to take out the web log sub-community. It has been tested for terrorist network to determine the threat levels regarding the vigor of communication inside the society and content expansion.

Jennifer Jie Xu and Hsinchun Chen [19] recover the effectiveness of the current link examination software by offering a visual demonstration of a criminal network and also deploys shortest path algorithm to rapidly progress the investigation task. The data set is taken from Phoenix police branch from which the route recognized are significant 80% of the time and offers a great answer to the dilemma of recognizing the most powerful criminal associations among two or more units.

B. Node Discovery Problem

Criminal network analysis other major purpose is investigating the covert networks to answer the node detection issue.

Yoshiharu Maeno [20] offer two approaches to solve the node detection issue. The first approach is a heuristic method in which proximity metric is resolute deploying Jaceard's co-efficient and the other is k-medoids which is used for categorization of nodes. Aligned with these, the ranking algorithm is additionally deployed to improve the doubtful observation logs. The second approach is statistical inference method that deploys the maximal possibility approximation to understand the topology of the network, and uses an anomaly detection technique to recover the suspicious surveillance logs. The researchers deploy a computationally created network and global mujahedeen organization to make the test dataset for which the performance assessment is done.

Matthew Dombroski, Paul Fischbeck and Kathleen M. Carley [21] argue the potential of deploying the intrinsic arrangements experienced in social networks to create forecasts of networks deploying incomplete and absent information. The model is based on experiential network data showing the structural specifications of triad closure and adjacency.

C. Dynamic Network Analysis

Traditional investigation methods, such as Social Network Analysis (SNA) and link analysis are incomplete in their capability to make multiplex, multimode, large scale dynamic data that are required to typify terrorist networks. Therefore, to answer this issue, a modern method captioned as Dynamic network analysis (DNA) is initiated which not only supports the compilation, investigation and perceptive of the network but also forecasts the dynamic association and the impact of such dynamics on individual and group behavior.

Ian A. McCulloh and Kathleen M. Carley [22] argue about social network change discovery deploying statistical process control chart that notices when important alters happen in the network and from the chart a variety of centrality factors are computed for numerous consecutive time periods. The suspected time period when a alter has happened is investigations deploying CUSUM statistics and in depth time period is concerned for sympathetic the level of modification.

Kathleen M. Carley [23] develops an approach to approximate vulnerabilities and the effect of removing those vulnerabilities in covert networks. Key characteristics of this research contains: deploying detailed network data to assist associations to make an integrated image deploying network measures and using multi-agent simulation to forecast alters in the previously determined network sight over time. Vagueness is administered by running the model in a Monte-Carlo fashion to establish the strength of the results and examining the consequence by adding up and reducing nodes and edges in the fundamental networks.

D. Key-Player recognition and Sub-Group discovery

To execute any terrorist action there need to be some teamwork among the terrorist and these ties are frame around some nodes which act as main nodes or leaders who manage and command the movement of the group. There are plenty of works performed to learn about how the network is influenced if the key nodes are detached. These networks are alienated into subgroups and sympathetic this arrangement assists to interrupt terrorist network and expand efficient control policies to battle terrorism. Therefore, key player recognition and sub-group discovery are some main trouble in criminal network investigation.

Shou-de Lin and Hans Chalupsky [24] concentrate on investigating irregular examples in multi-relational networks (MNR) which deploys unverified framework to model semantic profile and finds the doubtful node with the abnormal semantic profile. The researchers suggest a new clarification apparatus that eases confirmation of the exposed results by producing human comprehensible natural language clarifications defining the sole characteristics of these nodes.

Nasrullah Memon, Nicholas Harkiolakis and David L. Hicks [25] have used the investigative data mining approach to learn terrorist networks deploying descriptive and predictive modeling based on centralities and used it to the discovery of high value people by investigating the effectiveness after eliminating some nodes, stablishing how many nodes are reliant on one node and if hidden hierarchy

exists discover the command structure. The researchers in this study have established this also recently defined approach with a case study of 7/7 bombing plot.

E. CAN for Homeland Security

Sudhir Saxena, K. Santhanam, Aparna Basu [26] has expanded in-house Terrorism Tracker (or T2) which implements systematic investigation for information on terrorist events from open sources. This paper tackles organization-to-organization connections of terrorist associations working in the Indian State of Jammu & Kashmir. The SNA software package, Visone, expanded in Germany, has been deployed with the T2 generation of "co-occurrence" pairs where associations are cited jointly in an event throughout the period 2000 – 2003. This output was rehabilitated into an adjacency matrix to shape the input to Visone for investigation and creation of connection graphs.

F. Counter Terrorism

Uffe Kock Wiil, Nasrullah Memon and Jolanta Gniadek [15] offer the Crime Fighter toolbox for counter terrorism which conducts a variety of procedures like data acquisition, knowledge management and information processing deploying a quantity of tools that are classified as semi-automatic tools which are web harvesting tool, data mining tool, data conversion tool, SNA tools, visualization tools and manual tools like knowledge base tools and structure analysis tools.

Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann [27] argue how terrorists share their ideology and communicate with members on the "Dark Web" the overturn side of the Web deployed by terrorists. To recover sympathetic of terrorist behaviors from the web, the information is composed deploying searching, browsing and crawling. Next, it is filtered based on domain and linguistic information. These are then investigated as domestic and international terrorism based on the group profile, dynamics and relations. It's been used for gathering and investigating information of 39 Jihad web sites.

4. Crawler based Search Engine to Support Terrorism Web Mining

Many scholars have immense concentration to criminal network investigation. The preceding researches [3] have illustrated an effectual employ of data mining approaches to demonstrate the criminal connections from a great volume of occurrence reviews by police departments. These use co-occurrence frequencies to determine correlations between pairs of criminals [2] shows a method to pull out criminal networks from websites which is delivered blogging services all over a topic-specific investigation devices. In addition, they classify the performers in the network in their approach by utilizing web crawlers that examine blog subscribers. Blog subscribers are contributed in a discussion associated to some criminal topics. When the network is built, some text organization techniques are utilized to evaluate the content of the documents. Therefore, a visualization of the network is suggested to social network view or concept network view [2].

Al-Zaidy et al [4] did a study that is dissimilar in three aspects. First, they attempt on formless textual data which are attained from a uncertain hard drive more freely than a well-structured police database. Consequently, this technique can establish publics of unidentified size, that is not limited to the pairs of criminals. Furthermore, the latter's approaches also categorize indirect relations while the most of previous studies recognize categorized relationships.

A social network paradigm is followed by criminal network. Therefore, the recommended method for social network analysis can be used in criminal networks. Many researchers have been conducted on the different methods which can be used to build a social network from text documents. Jin et al [5] planned a framework to take out social networks from text documents accessible on the web. A technique has been affirmed by [6] to grade firms based on the social networks extracted from Webpages. Mainly, these approaches are dependent on web mining techniques that are searched for the actors in the social networks from web documents. Other social network studies are focused on some type of text documents such as e-mails.

Zhou et al [7] future a probabilistic method that categorizes groups in email messages and pull out the association information by using semantics to label the relations. Alternatively, the technique is only applicable for e-mails and the users of the network are limited to the recipients and researchers. In the knowledge discovery pasture, experts have offered some approaches to assess the relations of terms in the textual background in a scientific context. A perception of association graph-based loom to investigate was developed by Jin et al [8] across a set of documents that connects two given topics. [9] The suggestions of the open and closed finding algorithms is to find and show evidence pathways that are between two topics, these two can be take place in the document set and it is not essentially to be in the same document. [10] In order to search for keywords that the users need, the open finding approach are used and bring back documents comprising related topics. Moreover, they utilize clustering techniques to evaluate the results and give the operator clusters of new information, this new information are related in concept of the initial request terms. Therefore, in

order to improve the results of web queries, this open discovery approach explore for new links between concepts. On the contrary, this paper concentrates on extracting web published textual documents and information from criminal network sites for research.

A framework of web crime mining was suggested by Javad et al [1] that is comprised of two parts. First, some pages under attack crime are fetched. Second, the content of pages is mined and analyzed (Fig. 1 has shown a sequential crawler). Actually, a crawler fetches some pages that are related to the crimes. Formerly, crawler fetched pages at a time, which was useless and the resource was wasted. The suggested model expected to stimulate proficiency by threads, multiple procedures, and asynchronous access to resources.

Crawlers can be a graph search algorithm which is used in webs, in this case, webs can be considered as a large graph in pages that can be shown as its hyperlinks and nodes as its edges. In the web pages surfing, a crawler first searches a few of the nodes and then searching the edges, and it stretches to other nodes. The procedure of fetching a page and exploring the connections is similar to growing a node in graph search. The entire procedure is based on the frontier and frontier is based on a data structure that offers lists of URLs unvisited pages to the crawler. Crawlers stored the frontier in the main memory to help the procedure be more effective. However, the following points should be considered. Through the decreasing price of memory, a large frontier size is observed. Therefore, when the frontier is filled, the crawler designer should categorize the URLs with low priority to be removed. In addition, note that the frontier is possible to fill quickly because the size is maximized. However, another significant point is that the sequence of extracting the URLs should be pre identified. Actually, the algorithm should be able to identify the sequence of URLs.

In this study the whole process initiates with a list of unvisited URLs that are named the frontier. Essentially, the frontier is an significant queue and due to its sensitivity, it is deployed in grading pages. The list of URLs comes from the seed URLs that a consumer prepares. Making the URLs provides the possibility to every main loop, the crawler pick URL from the frontier. Then, the page associated to the URL is fetched using HTTP. Throughout fetching the page, the saved page is investigated which URLs is pulled out and after that innovation exposed URLs added to the frontier. Consequently, the page or other extracted information not connected with the targeted terms that are reserved in a local disk sources.

Extinction of swarming can be conducted in numerous forms. In one case, the swarming ends once the proposed quantity of pages is crawled. Besides that, the procedure can be pressed to be finished because of the frontiers' getting empty. Though, this situation is not probable to occur due to the elevated average quantity of links.

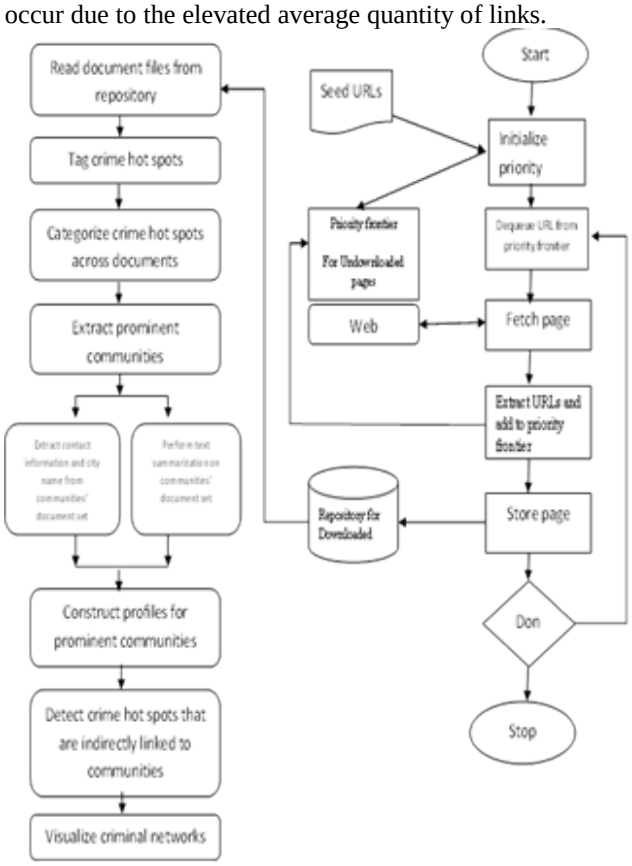

Fig. 1 Combined Websites and Textual Document Framework (CWTDF) for Criminal Network Mining

5. Limitations and Future Directions

The major restriction of social network investigation is the same that uses to any novel and inventive technology: social network investigation is just one instrument that can be deployed to appreciate terrorism, and is just one part of the puzzle. Subject matter specialists are required to provide a context for the research. Furthermore, the basic assumption of network analysis regarding terrorism may not be totally valid. In spite of their non-hierarchical method, terrorist associations are not totally prepared in a network structure. There are yet central headquarters and training amenities for most terrorist associations. In addition, social network investigation should challenge to tackle the fundamental root reason of terrorism. It is cooperative to appreciate how a network grows and how to undermine a network. It is more cooperative, though, to appreciate how networks recruit members and why people desire to join terrorist networks.

Data collection is hard for any network investigation since it is tough to make a total network. It is particularly difficult to attain information on terrorist networks. Terrorist groups do not offer information on their members, and the government hardly ever permits researchers to use their aptitude data. A number of educational researchers concentrate mainly on data collection on terrorist organization, investigating the information throughout explanation and simple modeling.

An ordinary issue for the modelers is the matter of data. Any educational work is merely as good as the data, no substance the kind of superior approaches deployed. Modelers frequently do not have the most excellent data, as they have not gathered individual biographies (like Sageman) and do not have admission to confidential data. Many of the approaches are made data-free or without whole data, still do not completely believe human and data restrictions. The suggestion of this is that the outputs can be potentially misleading, as they cannot consider behavioral and related problems that might influence the network arrangement and activity. For instance, it would be moderately hard to model the network arrangement and progression of al Qaeda because many of the associations that maintain ties to al Qaeda are lying and do not really have those ties. It can be relatively hard distinguishing these groups from other, truthfully insecurely affiliated groups.

Additionally, modelers frequently do not have a basis in terrorist investigations nor do they always work with top counter-terrorism specialists. Without the assist of counter-terrorism specialists or a backdrop in terrorism researches, it is hard to turn the quantities and graphic models into visible results that create sense in the background of the enormous literature on terrorism.

For future studies, we recommend some effective algorithms for various components of the framework that are indicated in this article, for example, An Enhanced Ontology-based Crime Web Miner Algorithm for crawling the web contents and importing different types of crime ontologies to find out the suspicious or malicious crimes. In that case, combining an effective and existing crime web miner algorithm with semantic Web and specifically OWL (as a Web Ontology Language) might be taken into account. As a result, a prototype uses Java programming to support the applicability of the proposed framework and the evaluation of the result of the proposed approach with other current approaches to determine the effectiveness of the approach will be conducted.

6. Conclusion

The assessment of the recovered information and supporting the study process can be conducted by reviewing of files that is engage seeking content for knowledge and information it means that reviewing suggest and tackle other information sources which stands on the ways that the researcher deployed for searching proof. In this research, the major goal is to viaduct the gap among formless text data and criminal network mining. Therefore, the issue is that the mining criminal communities from a set of text files have been gathered from a suspect's data. Conversely, in a "Text files" such as blogs, chat logs, web pages, e- mails, or any textual data, researchers attempt to execute some other search approaches to take out and categorize suitable information from the text due to its formless nature, and next for additional examination, enter the appropriate pieces into a well-organized database manually. Therefore, this manual procedure is error prone, time overwhelming and uninteresting and in addition the excellence of an investigation and the breadth of a search pretty much relies on the researcher's expertise and knowledge.

This study suggests an incorporated framework for assessing the criminal suspect forensic data investigation based on prioritize the web scale frontier efficiently and competently. Earlier researches on criminal network investigation primarily concentrate on investigating links among criminals in organized data or meager text documents. This study has initiated the framework in two parts. The first part extracts pages connected to crimes, and the second part parse and mines contents of famous pages based on grade. For future researches, we suggest the appearance of some efficient algorithms for a variety of parts of the framework shown in this paper for instance, an improved ontology-based crime Web miner algorithm for fetching and parsing of the pages from the Web and even the separation of the tools to recognize criminal networks as opposite to current ones.

Acknowledgments

This research is funded by the Zahedan Branch in Islamic Azad University, Zahedan, Iran. The authors would like to thank the Research Management Centre of Islamic Azad University-Zahedan Branch and cooperation including students and other individuals who are either directly or indirectly involved in this project.

References

[1] Hosseinkhani. J, Chaprut. S and Taherdoost. H. Criminal Network Mining by Web Structure and Content Mining. 2012.11th WSEAS International Conference on Information

Security and Privacy (ISP '12), Prague, Czech Republic September 24-26.
[2] Hosseinkhani, Javad, Suriayati Chuprat, and Hamed Taherdoost. "Discovering criminal networks by web structure mining." In Computing and Convergence Technology (ICCCT), 2012 7th International Conference on, pp. 1074-1079. IEEE, 2012.
[3] Chen H, Chung W, Xu JJ, Wang G, Qin Y, Chau M. Crime data mining: a general framework and some examples. Computer 2004; 37(4):50–6.
[4] Al-Zaidy, R. F., Benjamin C.M.; Youssef, Amr M ; Fortin, Francis . Mining criminal networks from unstructured text. documents." Concordia Institute for Information Systems Engineering, Concordia University, 1455 De Maisonneuve Blvd. West, CIISE (EV7.640), Montreal, QC H3G 1M8, Canada . 2012: 8: 147-160.
[5] Hope T, Nishimura T, Takeda H. An integrated method for social network extraction. In: Proc. Of the 15th international conference on world wide web (WWW); 2006. p. 845–6.
[6] Jin W, Srihari RK, Ho HH. A text mining model for hypothesis generation. In: Proc. Of the 19th IEEE international conference on tools with artificial intelligence ICTAI; 2007. p. 156–62.
[7] Zhou D, Manavoglu R, Li J, Giles CL, Zha H. Probabilistic models for discovering e-communities. In: Proc. of the 15th international conference on world wide web (WWW); 2006. p. 173–82.
[8] Jin Y, Matsuo Y, Ishizuka M. Ranking companies on the web using social network mining. In: Ting IH,Wu HJ, editors.Web mining applications in e-commerce and e-services. Studies in computational intelligence, vol. 172. Berlin/Heidelberg: Springer; 2009. p. 137–52.
[9] Srinivasan P. Text mining: generating hypotheses from medline.Journal of the American Society for Information Science and Technology 2004; 55:396–413.
[10] Skillicorn DB, Vats N. Novel information discovery for intelligence and counterterrorism. Decision Support Systems 2007; 43(4): 1375–82.
[11] Karthika, S., and S. Bose. "A comparative study of social networking approaches in identifying the covert nodes." International Journal on Web Services Computing (IJWSC) 2 (2011): 65-78.
[12] Peng Tao, "Research on Topical Crawling Technique for Topic- Specific Search Engine," Doctor degree thesis of Jilin University, 2007.
[13] Jennifer Schroeder, Hsinchun Chen, Jennifer Xu and Michael Chau "Automated criminal link analysis based on domain knowledge," Journal of the American society for information science and technology, vol. 58, no.6, pp. 842-855, (2007).
[14] Dombroski, M., P. Fischbeck, and K. Carley, "Estimating the shape of covert networks," presented in the proceedings of 8th International Command and Control Research and Technology Symposium, Washington, DC, June (2003).
[15] Uffe Kock Wiil, Nasrullah Memon and Jolanta Gniadek "Knowledge management processes, tools and techniques for counterterrorism," presented in the International conference on Knowledge Management and Information Sharing, pp. 29-36, (2009).
[16] Hosseinkhani, Javad, Suriayati Chuprat, Hamed Taherdoost, and Amin Shahraki Moghaddam. "Propose a framework for criminal mining by web structure and content mining." Information Technology (IJACSIT) 1, no. 1 (2012).
[17] Linton C. Freeman "Centrality in Social Networks Conceptual Clarification," Social Networks, vol.1, pp. 215-239, (1978/79).
[18] C. C. Yang and T. D. Ng, "Terrorism and crime related weblog social network: link, content analysis and information visualization," presented in IEEE international conference on intelligence and security informatics, New Brunswick, NJ, (2007).
[19] Xu J. J., Chen H., "Using shortest path algorithms to identify criminal associations," Decision Support Systems, vol. 38, pp. 473-487, (2004).
[20] Yoshiharu Maeno and Yukio Ohsawa "Analyzing covert social network foundation behind terrorism disaster," Int. J. Services Sciences, vol. 2, no. 2, (2007).
[21] Dombroski, M., P. Fischbeck, and K. Carley, "Estimating the shape of covert networks," presented in the proceedings of 8th International Command and Control Research and Technology Symposium, Washington, DC, June (2003).
[22] Ian A. McCulloh and Kathleen M. Carley "Social network change detection," Carnegie Mellon University, School of Computer Science, Technical Report, CMU-CS-08-116.
[23] Carley, K. M. "Estimating vulnerabilities in large covert networks," presentedin the proceedings of 9th International Command and Control Research and Technology Symposium held at Loews Corornado Resort, CA. Evidence Based Research, Vienna, VA, (2004).
[24] Shou-de Lin and Hans Chalupsky "Discovering and explaining abnormal nodes in semanticgraphs," IEEE Transactions on knowledge and data engineering, vol. 20, no. 8, pp.1039-1052, (2008).
[25] Nasrullah Memon, Nicholas Harkiolakis and David L. Hicks "Detecting High-Value Individuals in Covert Networks: 7/7 London Bombing Case Study," in the proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, pp. 206-215, (2008).
[26] Sudhir Saxena, K. Santhanam, Aparna Basu "Application of Social Network Analysis (SNA) to terrorist networks in Jammu & Kashmir," Strategic Analysis, vol. 28, no.1, (2004).
[27] Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann "Uncovering the dark web: A case study of Jihad on the web," Journal of the American society for information science and technology, vol.59, no.8, pp.1347–1359, (2008).