Detecting Terrorist Activity Patterns Using Investigative Data Mining Tool

Nasrullah Memon
Software Intelligence Security Research Center
Department of Software and Media Technology
Aalborg University
Niels Bohrs Vej 8, DK-6700 Esbjerg Denmark
nm@sis-rc.org

ABSTRACT

Law enforcement agencies across the globe have begun to focus on innovative knowledge discovery technologies to aid in the analysis of terrorists' information. The use of such technologies serves as intelligence tools to combat terrorism by predicting terrorism activity.

As opposed to traditional data mining aiming at extracting knowledge form data, mining for investigative analysis, called Investigative Data Mining (IDM), aims at discovering hidden instances of patterns of interest, such as patterns indicating an organized crime activity. An important problem targeted by IDM is identification of terrorist networks, based on available intelligence. We present an approach to an IDM solution of this problem, using semantic link analysis and visualization of findings. The approach is demonstrated in an application by a prototype system. The system finds associations between terrorist and terrorist organizations and is capable of determining links between terrorism plots occurred in the past, their affiliation with terrorist camps, travel record, and funds transfer, etc. The findings are represented by a network in the form of an attributed relational graph (ARG). Paths from a node to any other node in the network indicate the relationships between individuals and organizations. The system also provides assistance to law enforcement agencies, indicating when the capture of a specific terrorist will likely destabilize the terrorist network.

In this paper we discuss this important application area, relate it to existing database technology and suggest how this technology should be extended to provide more appropriate facilities. We describe what we regard as an important new type of approaches, i.e. *subgraph retrieval facilities*, and present a demonstrator that we have implemented.

Keywords: Investigative Data Mining, iMiner, terrorist networks, visualization, social network analysis

1. INTODUCTION

When intelligence analysts are required to understand a complex uncertain situation, one of the techniques they often use to simply draw a diagram of the situation. The diagrams are attributed relational graphs, an extension of the abstracted directed graph [1]. In these graphs, nodes represent people, organizations, objects, or events. Edge represents relationship like interaction, ownership, or trust. Attributes store the details of each node and edge, like person's name, or interactions time of occurrence.

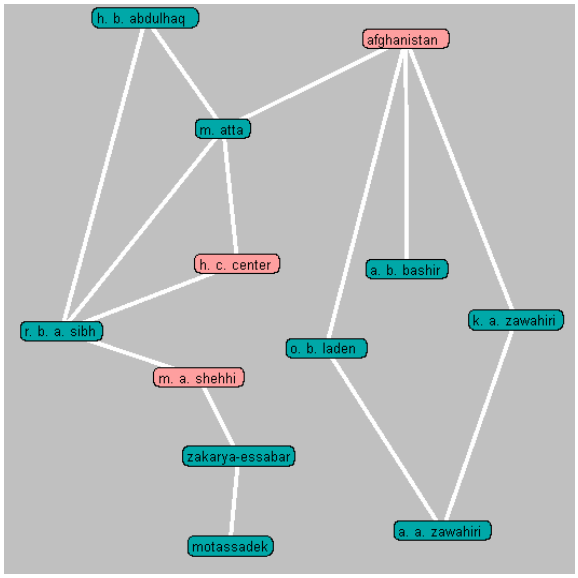

Fig 1: The connection between a set of people displayed as network

The graphs function as external memory aids, which are crucial tools for arriving an unbiased conclusion in the face of uncertain information [2] For example, if we have information that Osama-bin-Laden is a friend of Ayman-al-Zawahiri, who is father of Khalid-al-Zawahiri, who frequents at Al-Qaeda House Afghanistan, as does Abu-Bakar-Bashir, Hud-bin-AbdulHaq and Muhammad Atta who works at Hay Computing Service Hamburg, where he has a colleague Ramzi-bin-al-Sibh who provided funds to Marwan-al-Shehhi who is friend of Zakarya-Essabar who is brother of Mounir-al-Motassadek, then this information may be presented as in Figure 1.

Visualizing the connections in this way is of importance in investigating of terrorist networks. It has been found to aid considerably a good understanding of what is known so far, which is necessary to guide and direct further lines of inquiry in the most timely and productive way.

The study of terrorism networks fall into the larger category of criminal intelligence analysis, which is often applied to investigations of organized crimes (for example, terrorism, money laundering, fraud, etc.). Unlike other types of crimes often committed by single or few offenders, organized crimes are carried out by multiple, collaborating offenders, who may form groups and play different roles. In terrorist network, for example, different groups may be responsible for choosing venue to attack; some groups may be responsible for finding some sources of getting money (e.g. handling drug supply, distribution, sales, smuggling, and money laundering), some groups may be responsible for recruit people and some groups may be responsible for making bombs, etc. In each group there may be a *leader* who issues commands and provides steering mechanisms to the group, as well as *gatekeepers* who ensure that information flow effectively to and from other groups. Criminal intelligence analysis therefore requires the ability to integrate information from multiple crime incidents or even multiple sources and discover regular patterns about the structure, organization, operation, and information flow in criminal networks.

To disrupt criminal networks, both reliable data and sophisticated techniques play a central role. However, intelligence and law enforcement agencies are often faced with the dilemma of having too much data collected from multiple sources: bank accounts and transactions, phone records, vehicle sales and registration records and surveillance reports to name a few [3, 4], which in effect makes too little value, because they lack sophisticated network analysis tools and techniques to utilize the data effectively and efficiently.

Today's criminal intelligence analysis is primarily a manual process that consumes much human time and efforts, thus has limited applicability to crime investigation. Our objective is to provide an investigative data mining perspective for terrorist network analysis. We discuss challenges in data processing, review existing network analysis and visualization tools and recommend Social Network Analysis (SNA) approaches. Although SNA is not traditionally considered as data mining technique, it is especially suitable for mining large volumes of association data to discover hidden structural patterns in criminal networks [3, 4].

The remainder of the paper is organized as follows: Section 2 introduces criminal intelligence analysis and visualization tools; Section 3 presents IDM perspective of terrorist intelligence analysis and reviews some SNA techniques; Section 4 describes iMiner research test bed and introduces new algorithms for subgraph retrieval facilities and presents a demonstrator that we have implemented. This Section also discusses need of building database for gathering of network intelligence and Section 5 provides conclusion of this paper.

1.1 Challenges in Data Processing

Like data mining applications in many other domains, mining law enforcement data involves many obstacles. First, incomplete, incorrect, or inconsistent data can create problems. Moreover these characteristics of criminal networks cause difficulties not common in traditional data mining applications:

Incompleteness. Criminal networks are covert networks that operate in secrecy and stealth [5]. Criminals may minimize interactions to avoid attracting police attention and their interactions are hidden behind various illicit activities. Thus data about criminal networks is inevitably incomplete; i.e. some existent links or nodes will be unobserved or unrecorded [4].

Incorrectness. Incorrect data regarding criminals' identities, physical characteristics, and addresses may result either from unintentional data entry errors or from intentional deception by criminals. Many criminals lie about their identity information when caught and investigated.

Inconsistency. Information about a criminal who has multiple police contacts may be entered in law enforcement databases multiple times. These records are not inevitably consistent. Multiple data records could make a single criminal appear to be different individuals. When seemingly different individuals are included in a network under study, misleading information may result.

Problems specific to criminal network analysis lie in data transformation, fuzzy boundaries, and network dynamics:

Data Transformation. Network analysis requires that data be presented in a specific format, in which network members are represented by nodes, and their associations or interactions are represented by links. However, information about criminal associations is usually not precise in raw data and transforming them to the required format can be fairly labor-intensive and time-consuming.

Fuzzy boundaries. The boundaries of criminal networks are quite ambiguous. Even organized crime families are often interrelated and many significant crime figures

are significant precisely because they are connected to a number of different criminal organizations. It can be quite difficult for an analyst to decide whom to include and whom to exclude from a network under study [4].

Dynamic. Criminal networks are, for all practical purposes, are not static, but are subject to change over time (Each contact report, telephone call, or financial transaction has a time and date. The relationship between any two individuals is not merely present or absent (binary), it is simply weaker or stronger; rather it has a distribution over time, waxing and waning from one period to another. Many of most useful network questions depend heavily on this temporal dimension, begging information about which associations are becoming stronger, or weaker, or, extinct). New methods of data collection may be required to capture the dynamics of criminal networks [4].

Some techniques have been developed to address these problems. For example, to improve data correctness and consistency, many heuristics are employed in the FinCEN system as the U.S. Department of Treasury to disambiguate and consolidate financial transactions into uniquely identifies individuals in the system [6]. Other approaches like concept space method [7] can transform crime incident data into a networked format [8].

2. CRIMINAL INTELLIGENCE ANALYSIS AND VISUALIZATION TOOLS

Klerks [10] categorized existing criminal network analysis approaches and tools into three generations.

First Generation: Manual Approach. Anacapa chart [10] is the representation of first generation. With this approach, an analyst must first construct an association matrix by identifying criminal associations from raw data. A link chart for visualization purposes can then be drawn based on association matrix. For example, to map the terrorist network containing the 19 hijackers in 9-11 attacks, Krebs [5] gathered data about the relationships among the hijackers from publicly released information reported in several major newspapers. He then manually constructed an association matrix to integrate these relations [5] and drew a network representation to analyze the structural properties of network.

Although such a manual approach for criminal network analysis is helpful in crime investigation, it becomes an extremely ineffective and inefficient method when datasets are very large.

Second generation: Graphic-based approach. These tools can automatically produce graphical representations of criminal networks. Most existing network analysis tools belong to this generation. Among them Analyst's Notebook, Netmap and XANALYS Link Explorer (previously called Watson) [9], are the most popular. For example, Analyst's Notebook can automatically generate a link chart based on relational data from a spreadsheet or text file. Although second generation tools are capable of using various methods to visualize criminal networks, their sophistication level remains modest because they produce only graphical representation of criminal networks without much analytical functionality. They still rely on analysts to study the graphs with awareness to find structural properties of the network.

Third Generation: SNA. This approach is expected to provide more advanced functionality to assist crime investigations. Sophisticated structural analysis tools are needed to go from merely drawing networks to mining large volumes of data to discover useful knowledge about the structure and organization of criminal networks.

3. IDM PERSPECTIVE OF TERRORIST INTELLIGENCE ANALYSIS

When analyzing terrorist networks, terrorism investigators often focus on characteristics of the network structure in order to gain insight in the following questions:

- Who is important?
- Why is s/he important?
- What subgroups exist in the network?
- What are the patterns of interaction between subgroups?
- What are the various roles in the network?
- How can the law enforcement use (often incomplete and faulty) network data to disrupt and destabilize terrorist networks?
- How does information or goods flow in the network?

A clear understanding of these properties in a criminal network may help analyst target critical network members for removal or surveillance, and locate network vulnerabilities where disruptive actions can be effective. Appropriate network analysis techniques, therefore, are needed to mine criminal networks and gain insight into these problems.

SNA. Social network analysis (SNA) is the study of human social interaction. Graph representations are ubiquitous throughout SNA—sequences of interactions between people are usually represented as an ARG. SNA metrics quantify different aspects of the ARG's topology, and the metric values can be used to characterize the roles of individuals within a group, or the state of a group or organization as a whole. The key opportunity for intelligence analysis is that "normal" social interaction and the social interaction of illicit

groups tend to exhibit significantly different SNA metric values.

A "social network" is defined as a group of collaborating (and/or competing) entities that are related to each other. Mathematically, this is a graph (or a multi-graph); each participant in the collaboration is called an actor and depicted as a node in graph. Valued relations between actors are depicted as links between the corresponding nodes. Actors can be persons, organizations, or groups- any set of related entities.

The geodesic assumption and the redundancy assumption state that for human interaction, "People with strong relationships usually communicate via the shortest path" and "Normal social networks are redundant." Studies have shown that both of these assumptions are typically false for groups trying to hide their activities [1]. For those groups, information compartmentalization and robustness to the compromise of group members overrule the efficiency concerns that otherwise lead to the geodesic and redundancy assumptions. The resulting differences in the groups' structures can be quantified by SNA metrics.

The SNA theory of homophily argues that most human communication occurs between people similar to each other. Thus people pursuing illicit activities are likely to be found communicating with others pursuing illicit activities. This "relational autocorrelation" further drives these groups' SNA metrics toward anomalous values [13].

Our work combines SNA metrics to give the analyst a tool for automatically pinpointing suspicious group dynamics within large volumes of data [11]. This combination will yield algorithms that constantly scan incoming information, alerting the analyst to anomalous social patterns that might indicate threatening activity. Some illicit groups (for example, terrorist cells moving from a "sleeper" to an "active" state) finish in a relatively normal configuration, but the history of how they arrived there is highly abnormal [5]. Therefore, it is also important to develop techniques to classify activity based on the evolution of a group's SNA metric values [12]. Because analysts have imperfect visibility into these interactions, we must also consider the sensitivity of various SNA metrics to limited observability [14].

SNA is used in a wide range of applications, from analyzing relations within families [15] to analysis of a Military C4ISR (Command, Control, Communications, Computers and Intelligence, Surveillance, and Reconnaissance) networks [16]; from analyzing the positions of adolescents in social networks and their sexual experience [17] to analyzing political power networks [18]; from analyzing management structures in multi-national corporations [19] to analyzing terrorist network [20]. The website of association of researchers, ISNA [21], provides links to journals, mailing lists and other resources.

Subgraph isomorphism and statistical classification via SNA metrics are two important classes of techniques that operate on attributed relational graphs, a representation familiar to the intelligence analyst. These two techniques help the analyst solve one of today's most common intelligence problems: finding significant combinations of events in a deluge of information.

Centrality. It deals with the roles of individuals in a network. Several centrality measures, such as degree, betweenness, and closeness can suggest the importance of a node in a network [22]. The degree of particular node is its number of links; its betweenness is the number of geodesics (shortest paths between any two nodes) passing through it; and its closeness is the sum of all the geodesics between the particular node and every other node in the network. An individual's having high degree, for instance, may imply his leadership; where as an individual with a high betweenness may be a gatekeeper in the network. Krebs [5] found that in the network consisting of the 19 hijackers, Mohamed Atta scored the highest on degree and closeness, but not on the betweenness. In our recent published paper [30] we have used degree centrality [22] and Eigenvector centrality 31] to convert undirected graph to a directed graph then used an algorithm by which we created a hierarchy of terrorist network. The intelligence agencies may benefit from that hierarchy in capturing terrorists.

Implications. Effective use of SNA techniques to mine criminal network data can have important implications on crime investigations. For example, clustering with blockmodeling can help show the hidden structure of a criminal network. The knowledge gained may aid law enforcement agencies fighting crime proactively, for example, allocating an appropriate amount of police effort to prevent a crime taking place, or ensuring is carried out [5]. Sometimes, new structures discovered may even modify investigator's conventional views of certain crimes. For instance, Klerks [10] has found the stereotypical impression of hierarchical organizations within organized crimes is being replaced by an image of more fluid and flattened networks. Traditional police strategies targeting leaders of hierarchical criminal organization may have become less effective in fighting organized crimes today. The work by Krebs also demonstrates that the network consisting of 19 hijackers in the 9-11 attacks is fairly flat and dispersed [5]. The advantage of such a structure is an increase in the network's resilience and an emphasis on minimizing damage should some network members be captured or compromised.

SNA may also help address the challenge of data processing. Blockmodeling, for example can easily

detect "structural holes" [10] in which the link density is lower than a threshold density value. According to McAndrew [3] structural holes may indicate incomplete or missing data thereby drawing analyst's attention to further data collection and improvement.

Subgroup detection. A terrorist network can often be partitioned into cells (subgroups) consisting of individuals who closely interact with each other. Given a network, traditional data mining techniques such as cluster analysis may be employed to detect underlying groupings that are not otherwise apparent in the data. Hierarchical clustering methods have been proposed to partition a network into subgroups [22]. Cliques whose members are fully or almost fully connected can also be detected based on clustering results.

4. RESEARCH TEST BED

In this research and development study, we employed SNA techniques for terrorist intelligence analysis. The goal has been to provide law enforcement and intelligence agencies with third-generation network analysis techniques that not only produce graphical representations of terrorist networks but also provide structural analysis functionality to facilitate terrorist investigations. Our intension is also to introduce strategies to assist law enforcement and investigative agencies to disrupt terrorist networks.

The iMiner is an experimental system, which provides facilities for retrieval of information and its presentation in graph form. A number of facilities that enable small subgraphs to be retrieved and added to the browsing canvas are also provided. In the current implementation we have provided four such facilities that are described in next section.

4.1 The subgraph retrieval facilities.

The user begins to construct a view by placing one or more objects on the browsing canvas, either by selecting from the list of those stored, or by retrieving objects according to their attribute values. The user may then begin to use the facilities that we now describe using the example of the database shown in figure. 2.

4.1.1 Retrieving all objects that are directly or indirectly connected to a specified object

This facility may be used to retrieve and display all objects stored in the database that are connected an object already displayed on the browsing canvas by a path in the database of an arbitrary length, the associated connecting paths also being displayed. The user may specify the maximum length of a path from the object and the type of links that connecting path may include.

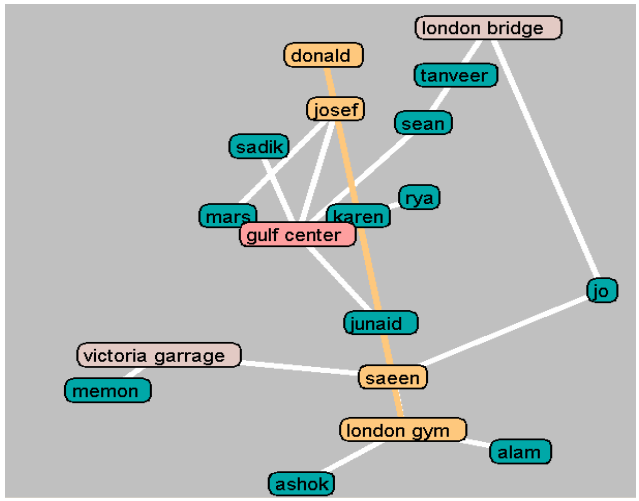

Fig. 2: A small terrorist intelligence database

For example, if an object represented *Saeen* was placed on the browsing canvas and this facility was used to display all objects connected to *Saeen* by a path of length two or less then the objects and links shown in figure 3 would be displayed.

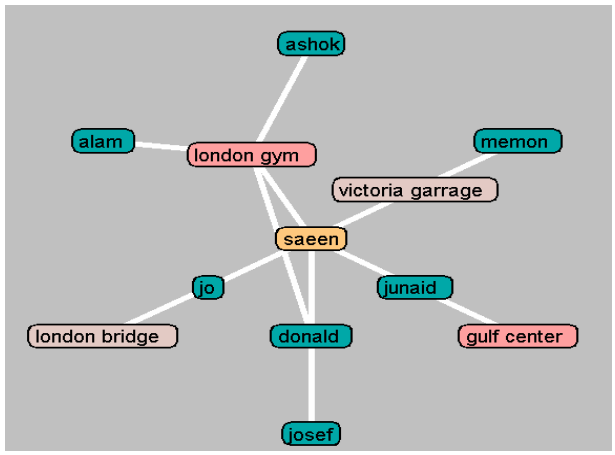

Fig. 3: Results of using subgraph retrieval facility at section 4.1.1.

4.1.2. Finding paths that connect two specified objects

If *Saeen* was to be charged with participating in a bombing plot and the police suspected that *Mars* was also involved, the investigative officer (s) would be likely to want to know if, and how, *Mars* and *Saeen* are connected. Paths in the database connecting two

specified entities already on the browsing canvas may be displayed using *all path facility* as shown in figure 4.

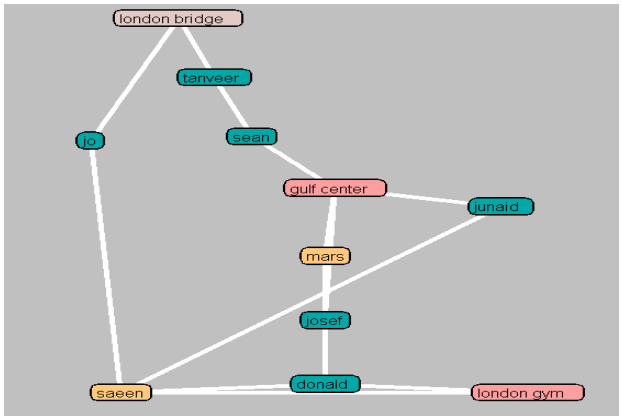

Fig. 4: The using all path facility to display all those paths in the database that is displayed in Fig. 2. that connect the objects representing *Saeen* and *Mars*.

The algorithm for all path facility is described as under:.

```
Algorithm
Input:      Root and destination nodes,
            Temp_list and Paths are linked lists
Output:     All Paths starting from destination and ending at destination

Initialize  Construct a path, which contains only root
            Add this path to Paths

            While Paths is not empty
                  Create new Temp_List.

                  For each path in Paths
                        Let n is leaf of path

                        For each edge coming from n
                              Let n_i is other nodeitem adjacent to current edge
                              If  n_i is not in current path
                                    Add the nodeitem to current path and save it
                                    to Temp_list
                              End if
                        End for

                  Mark n as visited
                  End for

            Save the paths leading to destination
            Set Paths=Temp_List
            End while
```

4.1.3. Finding connections between groups of objects

Consider the following witness statement, "I saw Alam and Memon in car with two other men. If Alam and Memon were two suspects in terrorist plot then police would like to identify the two other men. Support for finding connections between groups of objects is provided by this facility.
Consider the witness statement above, using this facility to retrieve objects that are instances of the person object class and connected to the objects Victoria Garage, Saeen, London Gym, and Donald as shown in figure 5. Thus, Saeen and Donald are identified as possible companions of Alam and Memon.

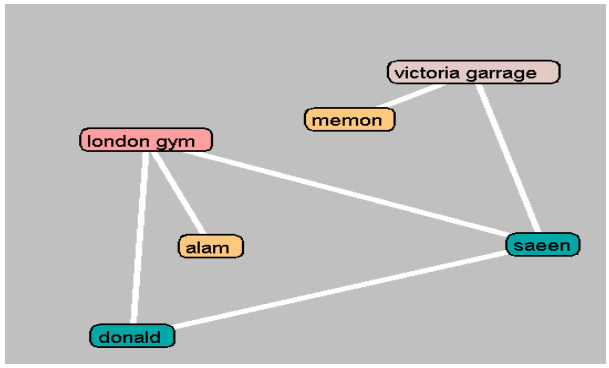

Fig. 5. The results of witness statement as at section 4.1.3.

The algorithm for this facility is shown in figure.

```
Algorithm
Input:      Root and destination nodes,
            Temp_list and Paths are linked lists
Output:     All shortest Paths starting from destination and ending at destination

Initialize  Construct a path, which contains only root
            Add this path to Paths

            While Paths is not empty
                  Create new Temp_List.

                  For each path in Paths
                        Let n is leaf of path

                        For each edge coming from n
                              Let n_i is other nodeitem adjacent to current edge
                              If  n_i is not visited
                              Add the nodeitem to current path and save it to
                              Temp_list
                        End for

                  Mark n as visited
                  End for

            Save the paths leading to destination
            Set Paths=Temp_List
            End while
```

4.1.4. Shortest Paths between root and destination

This facility includes all paths which are the shortest in length. It uncovers the entities between root and destination. The all paths yielded from above given algorithm are evaluated and shortest ones are only included. For example, if we use this facility for the example as mentioned in section 4.1.3., then shortest path between *Alam* and *Memon* are found, which exclude *Donald* from Fig. 5.

4.2 iMiner Knowledgebase and gathering of network intelligence

In the aftermath of the September 11th attacks, it was noted that coherent information sources on terrorism and terrorist groups were not available to researchers [23]. Information was either available in fragmentary form, not allowing comparison studies across incidents, groups or tactics, or made available in written articles - which are not readily suitable for quantitative analysis of terrorist networks. Data collected by intelligence and law-enforcement agencies, while potentially better

organized, is largely not available to the research community due to restrictions in distribution of sensitive information.

To counter the information scarcity, a number of institutions developed unified database services that collected and made available publicly accessible information on terrorist organizations. This information is largely collected from open source media, such as newspaper and magazine articles, and other mass media sources.

Such open-source databases include:

1. RAND Terrorism Chronology Database [24] - including international terror incidents between 1968 and 1997.
2. RAND-MIPT (Memorial Institute for Prevention of Terrorism) Terrorism Incident Database [25], including domestic and international terrorist incidents from 1998 to the present.
3. MIPT Indictment Database [26] - Terrorist indictments in the United States since 1978.

   Both RAND and MIPT databases rely on publicly available information from reputable information sources, such as newspapers, radio and television.

4. IntelCenter Database (ICD)[27] includes information on terrorist incidents, groups and individuals collected from public sources, including not only traditional media outlets and public information (such as indictments), but also information learned from Middle East-based news wire services.

   Separately, IntelCenter also collects information from Arabic chat-rooms and Internet-based publications - although value of such data is questionable and data may be tainted by propaganda.

The focus of these databases is the agglomeration of publicly available data and dissemination of it to researchers, both in the public and private sectors. Little of the work in large public databases has been focused on enabling social network analysis or link analysis of covert and terrorist networks. The IntelCenter Corporation has released a dataset mapping relationships between members of Al-Qaeda [28]. However, that dataset was delivered as virtually a read-only diagram that did not facilitate quantitative analysis of the data.

Furthermore, the data in the above databases is frequently presented in a proprietary format, making it difficult to employ other software for analysis purposes.

On the commercial software frontier, I2 Corporation has been marketing Analyst's Notebook [9], a software product for integrating and charting network-based intelligence on criminal and terrorist organizations. This software is in use in many governmental and law enforcement agencies, and allows significant integration with data collection, communication and other technologies. A separate product, iBase, provides shared storage and data integration facilities of the product. However, the product implements very few quantitative analysis tools and does not allow ready export of network data into analysis packages.

The goal of the iMiner knowledgebase is to provide a means for ready collection and integration of network data, with an emphasis on making the data available for quantitative analysis with standard software tools, and making the database accessible on the basis of open standards for database connectivity.

Storing and manipulating massive persistent graph data is a non-trivial preposition. Despite the fact that majority of data captured by businesses and organizations is relational in nature and can be efficiently described in terms of graphs, much of database and data mining research in the past decade has concentrated on propositional data [29].

In propositional data, instances and objects are assumed to be identical and independently distributed (*i.i.d.*). Relational data violates this assumption. Relationships among objects reflect dependence among instances, and the instances themselves are heterogeneous. Rich social network data, such as information extracted via text analysis, further supports this fact by attaching semantics and attribute sets to both instances and the relations themselves.

iMiner knowledgebase system is flexible for handling large volumes of graph-based and social network data. We believe that it provides a reliable means of storage and manipulation of graph based data.

6. CONCLUSION

In this paper we have discussed an important investigative data mining tool. The system discovers hidden instances of patterns of interest, such as patterns indicating terrorism activity. The system finds associations between terrorists and terrorist organizations and is capable of determining links between terrorist plots occurred in the past, their affiliations with terrorist camps, travel records and funds transfers, etc. The area of research is still in its infancy but we believe that intelligence agencies could be benefited.

We demonstrated our newly introduced algorithms for subgraph retrieving facilities. The main purpose of this research is to produce an investigative tool for visualization, analysis and destabilizing terrorist networks as well as to develop a flexible database

system for handling large volumes of graph-based social network data.

REFERENCES

[1] Coffman T., Greenblatt S., Marcus S. *Graph Based Technologies for Intelligence Analysis*. Communications of ACM. Volume 47 (3), 2004.

[2] Heuer, R.J. *Psychology of Intelligence Analysis*. Center for Study of Intelligence, Central Intelligence Agency, 2001.

[3] Mc Andrew, D. The structural analysis of criminal networks. *The Social Psychology of Crime: Groups, Teams and Networks, Offender Profiling Series, III.* D. Canter and L. Alison (Eds.) Aldershot, Dartmouth (1999).

[4] Sparrow, M. K. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks 13 (1991), 251-274.*

[5] Krebs, V. E. Mapping networks of terrorist cells. *Connections 24,3 (2001), 43-52.*

[6] Goldberg, H.G., and Senator, T.E. Restructuring databases for knowledge discovery by consolidation and link formation. *In Proceedings of 1998 AAAI Fall Symposium on Artificial Intelligence and Link Analysis.* AAAI Press (1998).

[7] Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., and Schroeder, J. COPLINK: Managing law enforcement data and knowledge. *Communication ACM 46,1* (Jan. 2003), 28-34.

[8] Xu, J., and Chen, H. CrimeNet explorer: A framework of criminal network knowledge discovery. *To appear in ACM Transactions on Information Systems*.

[9] Jesus M. Investigative Data Mining for Security and Criminal Detection. *Elsevier Science*, 2003.

[10] Klerks, P. The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* 24, 3 (2001), 53–65.

[11] Coffman, T. and Marcus, S. Pattern classification in social network analysis: A case study. In *Proceedings of the 2004 IEEE Aerospace Conference* (Big Sky, MT, Mar. 2004).

[12] Coffman, T. and Marcus, S. Dynamic classification of groups using social network analysis and HMMs. In *Proceedings of the 2004 IEEE Aerospace Conference* (Big Sky, MT, Mar. 2004).

[13] Jensen, D., Rattigan, M., and Blau, H. Information awareness: A prospective technical assessment. In *Proceedings of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2003.

[14] Thomason, B., Coffman, T., and Marcus, S. Sensitivity of social network analysis metrics to observation noise. In *Proceedings of the 2004 IEEE AerospaceConference* (Big Sky, MT, Mar. 2004).

[15] Wildmer, E.D., and La Farga, L., Boundness and Connectivity of Contemporary Families: A Case Stdy. *Connections* 22(2): 30-36 (1999)

[16] Dekker, A., Applying Social Network Analysis Concepts to Miltary C4ISR Architecture. *Connections* 24(3): 93-103 (2002).

[17] Ellen, J. M., Diolcini, M., Bir, N.D., Harper, G. W., Waston, S., and Valente, T., Social Network Centrality and Sexuality Experience Among Household Sample of Urban African-American Adolescents. *Connections* 24(2): 76-81 (2001).

[18] Mendieta, J. G., Schmidt, S., Aastro, J. and Ruiz, A. A., Dynamic Analysis of Maxican Power Network. *Connections* 20(2): 34-55 (1997).

[19] Athanassiou, N., International Management Research and Social Networks. *Connections* 22(2): 12-21 (1999).

[20] Van Meter, K. M., Terrorists/Liberators: Researching and dealing with adversary social networks, *Connections* 24(3): 66-78 (2002).

[21] INSNA, http://www.sfu.ca/~insna/

[22] Wasserman, S., and Faust, K. Social Analysis: Methods and Applications. *Cambridge University Press, Cambridge*, MA, 1994.

[23] Le Gruenwald, Gary McNutt, and Adrien Mercier. *Using an ontology to improve search in a terrorism database system*. Proceedings of the 14th International Workshop on Database and Expert System Applications (DEXA'03), 2003.

[24] RAND Corporation. Purpose and description of information found in the incident databases. http://www.tkb.org/RandSummary.jsp.

[25] Brian Houghton. *Understanding the terrorism database.* National Memorial Institute for Prevention of Terrorism Quarterly Bulletin, 2002

[26] Brent L. Smith and Kelly R. Damphousse. *The American terrorism study*: Indictment database, 2002.

[27] IntelCenter Corporation. Intelcenter database (icd). http://www.intelcenter.com/icd/index.html.

[28] IntelCenter.com. Mapping al-qaeda v1.0. www.intelcenter.com.

[29] J. Neville and D. Jensen. *Supporting relational knowledge discovery: Lessons in architecture and algorithm design*. Papers of the ICML 2002 Workshop on Data Mining Lessons Learned, 2002.

[30] Memon N. et al, Destabilization of Terrorist Networks, *WSEAS Trasactions on Computers*, Issue 11, Volume 4, November 2005, pp. 1649-1656.

[31] Bonacich, P. 1972. Factoring and Weighing Approaches to Status Scores and Clique Identification. *Journal of Mathematical Sociology:* 2: 113-120.