Using the Spanning Tree of a Criminal Network for Identifying Its Leaders
T.Jaishree¹, Dr.U.V.Arivazhagu M.E, Ph.d²
Professor and head²
Kingston Engineering College, vellore, India

Abstract:
We introduce a forensic analysis system that identifies the influential members of a criminal organization as well as the immediate leaders of a given list of lower-level criminals. Criminal investigators usually seek to identify the influential members of criminal organizations, because eliminating them is most likely to hinder and disrupt the operations of these organizations and put them out of business. We construct a network representing each criminal as a vertex. Vertices are ranked based on their scores. Criminals represented by the top ranked vertices are considered the influential members of the criminal organization represented by the network.

Index Terms: Forensic Investigation, mobile communication data, ECL finder, social network analysis

I. INTRODUCTION
Social group and their relationships have been identified using social network analysis (SNA). By using forensic investigation it is used for identifying criminal communities, their relationships, and influential leaders. Forensic investigators study and analyze communication records for the purpose of identifying criminal communities and the leaders. Mobile Communication Data (MCD) that belong criminal organisations to construct networks that depict the organisations and analyze these networks. Most criminals involved in terrorism, drug trafficking, and criminal gangs. Criminal forensic investigators analyze networks to infer useful information such as: (1) the structure of the criminal organisation, (2) the relationships between the criminals, (3) the influential members of the criminal organisation, (4) the flow of communication between the criminals. We propose in this paper a forensic analysis system called ECLFinder (Efficient Criminal Leaders Finder). It can identify the most influential members in the criminal organisation. ECLFinder constructs the minimum spanning tree (MST) of the network. In existing system detecting the top criminals are difficult and it’s depends upon the manual process. It takes plenty of time to find the top criminal if there is plenty of data. If we fail to eliminate the top criminal leader then the criminal organization will go stronger. Manual crime investigation process is not efficient in detecting the top criminal leader. In proposed system we are forming the network structure based on the crime investigation reports. We consider each criminal as a vertex and we connect each vertex with a link. We analyze the criminal investigation reports and find the top criminal based on analyzing all the criminals. We are forming a network interconnecting all the criminals the criminal with the top score will be considered as top criminal. The top influential leader can be found accurately.

II. BACKGROUND
A number of methods have been proposed for identifying the set of suspicious source nodes (e.g., fake followers, botnets, etc.) on a given criminal network. The authors of [1] investigated the network structure of Mafia syndicates by building two networks representing Mafia gangs operating in the North of Sicily. In the networks, a vertex represents an individual and an edge connecting two vertices represents the existence of at least one reciprocated phone call between the individuals associated with these vertices. The following are the objectives of the authors of [1]: (1) to understand the functional roles of the members of the Mafia syndicates, (2) to quantify the ability of a Mafia syndicate to react to police operations after the detention of some of its members, and (3) the resilience of Mafia syndicate to disruption caused by police operations. The authors of [10] presented LogViewer, a Web-based criminal network analysis framework to study combinations of geo-embedded and time-varying data sources like mobile phone networks and social graphs. LogViewer aims at: (1) identifying criminal behaviors and uncovering illicit activities, (2) investigating the centrality of vertices representing criminals, (3) studying the flow of information over time, and (4) determining the physical closeness effects on networks. In 2013, Catanese et al. [7] introduced an initial version of a system called LogAnalysis. In this initial version, the system was intended for forensic visual statistical analysis of mobile phone logs. The system helps in understanding the hierarchies within criminal organizations and discovering key and central members inside the organizations [7]. Despite the success of most current methods for identifying the vertices that are important to query vertices, these methods suffer incomplete contribution and inconsistent contribution. Incomplete contribution occurs, if some query vertices do not contribute to the overall relative importance value of a vertex. The inconsistent contribution occurs, if vertex query vertices contribute unequally to the overall relative importance value of a vertex. Let v be the current vertex under consideration. ECLFinder overcomes the problem of Incomplete Contribution by: (1) considering the importance of each query vertex to v, and (2) assigning a weight to each incoming edge to v that is outgoing from one of the query vertices (this weight represents the importance/rank of this vertex relative to all incoming edges to v). ECLFinder overcomes the problem of Inconsistent Contribution by: (1) considering the importance of each query vertex to each vertex connected to v, and (2) accounting for the degree of relativity of v to all query vertices.
III. SYSTEM ARCHITECTURE

The actors are informer, officer and public. The informer maintains criminal account which consists of criminal details we can add the list of criminals, we can activate for officer and it consists of officer details. The informer requests to the officer to register the details of the criminal and the officer responds to the informer. The officer maintains another criminal account with all the records in the database and all the details of the criminal are stored in the main server. The public can also store the details of the criminal in the database and the account is maintained. It consists of criminal details and the message is transferred from source to destination. Finally by using all these, the scores are given and the top ranked vertices are identified as influential leader in criminal organisation.

Figure 1. System architecture

IV. OUTLINE

1) Constructing a network: A network is constructed from either MCD associated with a criminal organization or crime incident reports that contain information about the members of a criminal organization.

2) Assigning a weight to each edge in the network: In a network constructed from MCD, the weight of an edge represents the number of phone calls/messages between two criminals. In a network constructed from crime incident reports, the weight of an edge represents the number of co-occurrences of the names of suspects and accomplices in the same reports.

3) Computing the shortest-path edge betweenness: We compute the “shortest-path edge betweenness” [11] for each edge based on the initial weights described in step 2. We replace edges’ initial weights by their shortest-path betweenness.

4) Assigning a score to each edge: Edges’ shortest-path betweenness are replaced by the inverses. This is because we will construct the MST of the network, which spans all vertices with the minimal sum of weights. The inverses are used as the scores of the edges.

5) Assigning a score to each vertex in the network based on the concept of existence dependency: We construct the MST of the network based on the edges’ scores described in step 4. ECLfinder assigns a score to each vertex v in the network. The score of the vertex v is the number of other vertices, whose existence in the MST is dependent on v. The score represents the relative rank (i.e., importance) of the criminal represented by the vertex v in the criminal organization.

6) Identifying the influential members of the criminal organization: Vertices are ranked based on their scores described in step 5. Criminals represented by the top ranked vertices are considered the influential members of the criminal organisation.

ALGORITHM

Prin’s algorithm: Algorithm CONSTRUCT-MST (NW, S, r)
1. for each u ∈ V [NW]
2. do key [u]←∞
3. π[u] ← NIL
4. key[r]←0
5. Q←V[NW]
6. while Q ≠ Ø
7. do u←EXTRACT-MIN(Q)
8. for each v∈Adj[u]
9. do if v ∈ Q and S(u, v) < key[v]
10. then π[v] ← u
11. key[v] ← S(u, v)
12. MST ← (v, π[v])

ECL FINDER: EFFICIENT CRIMINAL LEADER FINDER
To identify the influential members of the criminal organisation. It identifies the lower list criminals and identify the key nodes in the network.

SYSTEM ARCHITECTURE
The first step is Identification it identifies the incident and specify its type. The second step is Preservation it preserves and secure digital and physical evidence. The third step is Collection it document the crime scene and produce forensic copies of digital evidence. The fourth step is Examination and it includes In-depth examination and search of evidence and preparation of detailed documents for analysis. The fifth step is Analysis it filter and detect important data manually or through
analysis tools. The sixth step is Presentation it summarize and explain the conclusions.

AES SECURITY
AEIS a symmetric block cipher. It uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. Subordinate can only view symmetric block cipher. This means that it uses the same key for both encryption and decryption the data they want view or modify, download the data means they want to get the permission to superior. Here we implement AES superior data will be stored in encrypted format in database if user get response to data owner means they access the data at the time data will be automatically decrypt and display users.

MOBILE COMMUNICATON DATA(MCD)
It belongs to a criminal organisations or from crime incident reports that contain information about criminal network and tracks the calls of criminal members.

FINDING AN INFLUENTIAL LEADER
1. To find the Criminal records
2. Network auditor.
3. Criminal communication
4. Find criminal network

Criminal records
In this modules contain informer could be update every criminal details from cloud database. It means criminals which place they did misbehavior and their photo and every information they stored in database. Every day, thousands of crimes take place across the country. Behind every crime that is committed, lies the criminal who is capable of striking again anytime, anywhere. So we can find the criminal.

Network auditor
Audit/assurance review is to provide management with an independent assessment relating to the effectiveness of cybercrime prevention, detection and incident management processes, policies, procedures and governance activities. The review will focus on cybercrime management standards, guidelines and procedures as well as the implementation and governance of these activities. The audit/assurance review will rely upon other operational audits of the incident management process, configuration management and security of networks and servers, security management and awareness, business continuity management, information security management, governance and management practices of both IT and the business units, and relationships with third parties. IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process.

Criminal communication
The most appropriate criminal communication discussing trust in the context of organized crime, we would like to argue, is a network approach. We view trust first of all as a property of dyadic relations that form the basic elements of criminal networks. Criminal networks can be defined as sets of actors that are connected by ties which in some way or other support the commission of illegal acts. We find through the criminals which node they using in highest count.

Find criminal network
The first step in the analysis of a given criminal relation would be to examine whether or not trust user a role at all. The potential alternatives to trust are a relation characterized by either a lack of trust or by mistrust. Then criminal leader which node they communicated in most. Then we analysis the criminal leader.

V. LITERATURE SURVEY

Title: SIIMCO: A Forensic Investigation Tool for Identifying the Influential Members of a Criminal Organization

Author(s): Kamal Taha ; Paul D. Yoo
Members of a criminal organization, who hold central positions in the organization, are usually targeted by criminal investigators for removal or surveillance. This is because they play key and influential roles by acting as commanders, who issue instructions or serve as gatekeepers. Removing these central members (i.e., influential members) is most likely to disrupt the organization and put it out of business. Most often, criminal investigators are even more interested in knowing the portion of these influential members, who are the immediate leaders of lower level criminals. These lower level criminals are the ones who usually carry out the criminal works; therefore, they are easier to identify. The ultimate goal of investigators is to identify the immediate leaders of these lower level criminals in order to disrupt future crimes. We propose, in this paper, a forensic analysis system called SIIMCO that can identify the influential members of a criminal organization. Given a list of lower level criminals in a criminal organization, SIIMCO can also identify the immediate leaders of these criminals. SIIMCO first constructs a network representing a criminal organization from either mobile communication data that belongs to the organization or crime incident reports.

Title: Determining the Semantic Similarities among Gene Ontology Terms

Author(s): Kamal Taha

Published in: IEEE Journal of Biomedical and Health Informatics ( Volume: 17 , Issue: 3, May 2013 )
We present in this paper novel techniques that determine the semantic relationships among Gene Ontology (GO) terms. We implemented these techniques in a prototype system called GoSE, which resides between user application and GO database. Given a set S of GO terms, GoSE would return another set S’ of GO terms, where each term in S’ is semantically related to each term in S. Most current research is focused on determining the semantic similarities among GO ontology terms based solely on their IDs and proximity to one another in the GO graph structure, while overlooking the contexts of the terms, which may lead to erroneous results. The context of a GO term T is the set of other terms, whose existence in the GO graph structure is dependent on T. We propose novel techniques that determine the contexts of terms based on the concept of existence dependency. We present a stack-based sort-merge algorithm employing these techniques for determining the semantic similarities among GO terms. We evaluated GoSE experimentally and compared it with three existing methods.

Title: Collaborative Mining in Multiple Social Networks Data for Criminal Group Discovery

Author(s): Amin Milani Fard ; Martin Ester

Published in: Computational Science and Engineering, 2009. CSE ’09. International Conference on
Abstract: The hidden knowledge in social networks data can be regarded as an important resource for criminal investigations which can help finding the structure and organization of a criminal network. However, such network-based analysis has not been studied in an applied way and remains mostly a manual process. To assist inspectors and intelligence agencies, we define a new problem and then propose a framework for automated network data analysis and deduction approach from multiple social networks by converting to transaction datasets, applying association mining, and statistical methods. By applying a game theory concept in a multi-agent model, we try to design a policy for knowledge discovery and inference fusion.

Title: Novel intrusion detection system integrating layered framework with neural network

Author(s): Nidhi Srivastav; Rama Krishna Challa

Published in: Advance Computing Conference (IACC), 2013 IEEE 3rd International

The threat from spammers, attackers and criminal enterprises has grown with the expansion of Internet, thus, intrusion detection systems (IDS) have become a core component of computer network due to prevalence of such threats. In this paper, we present layered framework integrated with neural network to build an effective intrusion detection system. This system has experimented with Knowledge Discovery & Data Mining (KDD) 1999 dataset. The systems are compared with existing approaches of intrusion detection which either uses neural network or based on layered framework. The results show that the proposed system has high attack detection accuracy and less false alarm rate.

Title: Using GLIDER for Knowledge Discovery in Climate Science to Visualize, Analyze and Mine Satellite Imagery

Author(s): Sara Graves; Rahul Ramachandran; Todd Berendes

Published in: High Performance Computing, Networking, Storage and Analysis (SCC), 2012 SC Companion:

Satellite remote sensing provides an essential source of information for monitoring the earth’s atmosphere and climate. Thematic information derived from satellite imagery is applicable to a wide variety of applications at local, regional and global scales. Extracting thematic information using satellite imagery is a non-trivial task that usually requires preprocessing data by applying operations for radiometric and geometric corrections. Analysts need the ability to interactively apply different image enhancement operations to digitally enhance imagery, in order to identify subtle information that might be otherwise missed. Advanced algorithms are needed to allow users to analyze imagery and extract thematic information without having to alter the original data through geographic projections. The Globally Leveraged Integrated Data Explorer for Research (GLIDER) is an easy to use tool for visualization, analysis and mining of satellite imagery.

VI. RESULTS
### Figure 6. Officer Details Encryption

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Address</th>
<th>Mobile</th>
<th>DOB</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td><a href="mailto:john@gmail.com">john@gmail.com</a></td>
<td>1234 Main St, New York</td>
<td>123456</td>
<td>1/1/90</td>
</tr>
<tr>
<td>Sarah</td>
<td><a href="mailto:sarah@gmail.com">sarah@gmail.com</a></td>
<td>7890 Elm St, Los Angeles</td>
<td>67890</td>
<td>2/2/91</td>
</tr>
<tr>
<td>Michael</td>
<td><a href="mailto:michael@gmail.com">michael@gmail.com</a></td>
<td>4567 Oak St, Chicago</td>
<td>789012</td>
<td>3/3/92</td>
</tr>
</tbody>
</table>

### Figure 7. Officer Login Page

- Login: [Login Here]
- Mail Id: [123@gmail.com]
- Password: [enter]

### Figure 8. Registration Page of the Criminal by Officer

- Name: [Syed]
- Email: [sud@gmail.com]
- City: [Chennai]
- Postal Code: [600001]
- Mobile Number: [9876543210]
- Date of Birth: [12-12-1983]
- Sex: [Male / Female]
- Password: [enter]

FIGURE 9. OFFICER MAIN PAGE

FIGURE 10. CRIMINAL SEARCH PAGE

FIGURE 11. CRIMINAL DETAILS
FIGURE 12. ANALYSIS OF THE CRIMINAL BY RANKING AND SCORES

FIGURE 13. PUBLIC REGISTRATION
FIGURE 14. NETWORK PAGE

FIGURE 15. SOURCE TO DESTINATION

FIGURE 16. MESSAGE DISPLAY PAGE
VII. CONCLUSION

We introduced in this paper a forensic analysis system called ECLfinder. The system can determine the influential members of a criminal organization as well as the immediate leaders of a given list of lower-level criminals associated with the organization. First, ECL finder constructs a network representing a criminal organization from either MCD that belongs to the organization or from crime incident reports containing information about the organization. A vertex in such a network represents an individual criminal and an edge represents the relationship between two criminals. ECLfinder identifies the influential members of the criminal organization by determining the important vertices in the network representing the organization, using the concept of existence dependency. Hence by using the spanning tree the influential leader is identified and the criminal network is destroyed.

VIII. REFERENCES


