Criminal Network Visualization and Analysis using PEVNET

Fatima Nazir Rani, Muhammad Awais, Muhammad Yahya Saeed, Saba Nazir

Department of Software Engineering, Government College University, Faisalabad, Pakistan

Summary
The history of crime is as old as the existence of a human being. In past, the crimes were not organized enough and the criminal conspiracies were not much sophisticated as compared to this era we are surviving in. The evolutionary changes in human life have also influenced the patterns of criminal activities. The unprecedented technological capabilities combined with human creativity have given criminals a tremendous opportunity to create intractable criminal activities. The challenge is to inhibit exponential crime growth by identifying criminal mindsets plotting such heinous crimes. This research is carried out to address this dilemma of modern age through criminal network visualization and analysis. The research is stuffed with a real dataset used by Pakistan Police Department. This dataset contains detailed information on robbery crimes reported in January to July 2018. In order to achieve research objectives, data visualization and analysis is facilitated by a novel visualization technique called PEVNET. This research would help analysts and law enforcement agencies to examine the intensity of recent and to predict the magnitude of future crimes by visualizing and analyzing criminal networks.

Keywords:
PEVNET, Visualization and analysis, criminal networks, dataset

1. Introduction

Crime groups operate in criminal ecosystems that compose complex networks of interconnected and interdependent crime actions. They symbolize organic structures which transcend local, regional, national and policing frontiers, evolve over time and space and often disseminate their activities across different networks. Intelligence analysis includes the compilation of pieces of information to draw a clear picture of criminal networks on the canvas of visualization. The essentials for the extraction of core criminal network information includes, what is the flow of information in a network, who controls the network, what are their coordination patterns and how the information is executed and concealed in a criminal network. [1] The criminal networks evolve over time and their mutual relationships also alternate. Monitoring criminal networks are quite a challenging task because of the changing patterns of criminal groups and subgroups it becomes even more difficult to analyze their degree of violence. It demands an intellectual analyst collaboration to identify the central, most violent and the problematic criminal in a temporally evolving criminal network. There is sufficient evidence to prove that the temporal criminal networks are emerging day by day and accumulating other existing groups to form a huge criminal network. [2] The formulation of prevention strategies based on network visualization and analysis is the only solution to understand these meandering criminal networks that are filled with twist and fear. Criminal networks visualization and analysis can be helpful in isolating strengths and weakness of criminal networks that could resultantly enable law enforcement departments and surveillance agencies to dismantle and disrupt these networks. Criminal networks are a combination of dormant and influential actors. The influential actors are the key actors and dominate the whole network.[3] Identification of such powerful actors is mandatory to crack down the whole criminal network. A careful analysis and a strategic perception are fundamentally needed to collapse such criminal networks.

Knowledge of the structure and organization of the crime is significant for the investigation and the development of effective crime prevention strategies. The analysis of criminal networks is very critical and challenging as most of the information related to criminal networks are not easy to access. However, with the exception of preventing crimes, analysis of criminal data remains primarily a matter of concern. Modern methods of crime prediction do not provide a progressive structural analysis and crime forecasting which allow extraction of analysis for a given population. Predicting crimes has always been a problem for law enforcement agencies. Law enforcement bodies have formulated many legal policies to prevent criminal activities. In this reference, various attempts have been made to predict, detect and prevent crimes using various machine learning algorithms, including genetic algorithms, neural networks, clustering methods, data mining techniques, Bayesian networks, and decision trees. [4] Visualization provides information about the overall developmental scheme of criminal networks. Network visualization and analysis also help to conceptualize the crime patterns of criminals, committing crimes individually or in groups.

The purpose of this study is to equip analysts with solutions to combat crimes using an innovating visualization technique called PEVNET. The PEVNET tool will investigate and visualize the relationship between criminal groups. It would also provide a chance to make crime forecasts more detailed and specific. To make this research meaningful and result oriented, experimentation

Manuscript received October 5, 2018
Manuscript revised October 20, 2018

is performed on a real robbery crime dataset. One of the research objectives is to build a criminological profile on the basis of evidence classically suited to these robbery crimes. Modern criminologists and law enforcement agencies use criminal profiling to speed up the investigation method, which reviews strongest and weakest criminological ties to analyze the characteristics of the most likely suspects of a crime. [5] The profiling of offenders have successfully been practiced by the police department for decades. Although it is impossible to reflect all the characteristics and attributes of criminals, the analysis will be based on a real dataset entailing certain criminal prospects.

The structure of the remaining research paper is sequenced in a format outlined as follows. Section 2 includes the data collection strategies and the detailed literature that is reviewed to further this research. Section 3 outlines all the dynamics of the case study that is utilized to validate this research and to meet the anticipated research objective. Section 4 includes the discussion that describes and evaluates the results that are obtained after passing a set of inputs. Section 5 outlines the content that summarizes and concludes the paper.

2. Related Work

Table 1: Klerks in [2001] categorized the existing criminal network analysis tools into three generations.

#	*Generations*	*Visualization Technique Used*	*Type*	*Limitations*
1.	First Generation Approach also is known as Manual Approach (1975)	Anacapa Chart	Manual Visualization approach	Ineffective and inefficient for larger datasets
2.	Second Generation Approach also is known as Graphics-Based Approach.	Analyst's Notebook Netmap Watson XANALYS Link Explorer (Modified version of Watson)	Modestly sophisticated	Less structural capability Crime analysis burden remains on crime analysts
3.	Third Generation approach is also known as Structural Analysis Approach	CrimeNet Explorer a very few network visualization and analysis qualify for this generation of tools	More advanced, efficient and accurate	N/A

advantages, Netmap is very time-consuming in its usage capacity. [10][11] When there exist strong relationship among the group of criminals, CrimeNet characterizes these relations as thick links in a network. [4] Byron and Chen introduced COPLINK which integrates knowledge management techniques with investigative analysis (IA). COPLINK helps researchers for an easy exploration of suspects in a criminal network and it is also suitable for large-scale data networks. [12][6] Information seeking mantra by Schneiderman is also an effective visualization technique. The treemap algorithm by Shneiderman is mostly used for mapping social network information on a tree structure. [13] KeyPathwayMiner uses the Boolean matrix technique for the purpose of optimizing a visual query and it was proposed by Josch et al. [14] The CrimeFighter tool is used to counter terrorism. The CrimeFighter Investigator (CFI) is embedded in CrimeFighter. CFI contains some visualization features such as drag and drop and re-structuring. Crime Fighter Assistant and CrimeFighter Explorer are also some worth-mentioning visualization tools. [15][16][17] The network visualization tools are divided into three distinct generations by Klerks in 2001. [17] An overview of the tools of network visualization generations is shown in table 1.

Tulip is a simple and easy-to-use network visualization tool. But Tulip does not come with a great diversity of color schemes. Users have to change the color, shape, and size of nodes manually and to reload the status of the network. It takes a significant amount of time to change and edit the nodes in a large scale network. [18] Cytoscape offers support to all kinds of networks. Cytoscape does not provide raking and scaling of networks when the analysis of network data is performed. The clustering and layout routines require a significant amount of time in Cytoscape. [19] Pajek provides simple network visualization interface. Pajek-XXL, a special implementation of Pajek, extracts minor, most interesting and informative parts of a larger network which require further analysis and visualization using advanced tools.[20] The analysts assemble the pieces of information by utilizing different modes of information congregation. The information is sometimes managed by using compartmentalization technique and whiteboard analysis. Out of all the existing network visualization tools, no tool is sophisticated enough to visualize a complete and accurate information of criminal data in a network. Many tools support one or more data aspects and while others lack in other data aspects. Hence, there are multiple tools that are not up to the mark in one way or the other. A comparative analysis of existing visualization tools is described in table 2.

PEVNET is an IA tool that demonstrates its use in terms of visualization. PEVNET is actually the conversion of the investigation of crimes from the traditional methodologies of analyzing connections on the board to dynamic visualization. PEVNET simplifies investigation of crime procedures by providing comprehensive object information in a network. PEVNET is a novel visualization approach used for the visualization and the

analysis of criminal data in the form of a network. PEVNET has many new visualization functions that can help track the communication of individual criminal nodes to discover hidden patterns of criminal activity in subgroups. [9] PEVNET analyzes detailed data information to identify criminals. PEVNET is well suited for solving the problem of a multi-stage attack. In direct comparison with other classic modern tools, PEVNET has an improved overall performance and is much better at detecting complex intrusions.

Table 2: A comparative analysis of existing visualization tools

Evaluation Parameters	***Network Visualization Tools***				
	Cytoscape	***Gephi***	***Pajek***	***Tulip***	***PEVNET***
Scalability	●●	●●●	●●●●	●	●
Stability	●●●	●●●●	●●●	●	●●
Speed	●●	●●●	●●●●	●	●●●
Clustering	●●●●	●	●●	●●●	●●
Relevance to crime visualization and analysis	●●●●	●●●	●	●●	●
Level of memory efficiency	●	●●●	●●●●	●●	●●
Bundling of edges	●●●	●●	------	●●●●	●
Edge editing and manual node	●●●	●●●	●	●●●●	●●
Layouts	●●●	●●●●	●●	●	●●
Network profiling	●●●●	●●●	●	●●	●
Supported file formats	●●	●●●●	●	●●●	●●
Visual styles	●●●●	●●●	●	●●	●
User friendliness	●●	●●●	●●●●	●	●
Location Mapping	●	●	●	●	●
Filter based searching	●	●●	●	●	●
Modularity	●●	●	●	●	●●
Density	●●●	●●●	●●	●	●

● = Weaker; ●● = Medium; ●●● =Good; ●●●● = Strongest

PEVNET has several features, for example, discovering a co-operative sub-group feature, a similar node feature, a trend analysis feature, associate subgroups etc. PEVNET has a date filter menu which has a calendar of dates. The crime analysts can easily track criminal activity by using this feature. The next menu item is crime filter type, showing various types of crimes in a network. It can also find the geographical location of crime scenes by drawing a map. In order to detect changes in criminal activity during a certain period of time, the function of trend analysis is used. For example, the crime trend of all crimes registered in a year. This helps the analyst in forecasting and predicting certain criminal activities. With the help of such features, PEVNET provides a reliable platform for crime analysts. By using PEVNET tool, analysts can make operational decisions and easily perform their analysis in evaluation with other existing tools. PEVNET makes it easy to distinguish between sub-clusters that are problematic to perform in contrast to statistical methods and offers an enhanced interactivity. The PEVENT tool has already proved its worth in previous similar experiments. The results of these experiments were more accurate and as transparent as compared to any other modern tools e.g. Gephi, COPLINK, CrimeFighter, and KeyPathwayMiner. [5]

3. Case Study

It is important to identify vulnerabilities that exist in the prevalent security systems which could provide space to criminal networks to penetrate their roots deep enough to weaken the security and surveillance mechanisms. Loopholes in security systems lead to the manipulation of criminal networks. This research paradigm is intended to comprehend the criminal network dynamics in terms of visualization and analysis. In the course of this effort, a case study comprising robbery crime dataset is targeted. In this case study robbery crime dataset, used by the Pakistan Police Department, is applied to achieve research intentions. The research objective includes visualization, mapping, and prediction of crimes. It also surrounds the identification of crime and linkage patterns in a criminal network. This dataset contains the detailed information on robbery crimes reported in January to July 2018. The research is complemented by PEVNET tool that is used to visualize robbery crimes in the form of a network. The data is contained in MS Excel worksheets as it easy to maintain and understand data in this format. When analyzing criminal networks, characteristics and structure of the criminal network is mainly focused to gain an insight into the following research questions (RQs):

RQ1: What is the inclusive structure of the network?
RQ2: What are the linkage patterns between nodes in the network?
RQ3: Is it possible to map crime patterns in the network?
RQ4: Does PEVNET tool provide a basis for analyzing crimes in a way that leads to predict future crime?

In this research, a deliberate attempt is made to answer these research questions through data visualization and analysis. Network analysis gives information about criminal groups, subgroups and their subsequent chain of communication. To achieve this level of insight into the network, it requires examining the network structure

thoroughly. A high-level observation of network structure gives all the required evidence that is needed to satisfy the aforementioned research questions. Data analysis and visualization using PEVNET are discussed in an elaborative and comprehensive manner specifically focusing the RQs.

3.1 Examining the overall structure of the network

PEVNET tool has many innovative visualization features. The effective visualization of data helps in understanding the structure of a network. For the objective of understanding the network, the robbery dataset is visualized using PEVNET tool. PEVNET tools visualize the names of the offenders in the visualization stage. Initially, it provides an abstract view of the network. It automatically calculates the total number of nodes and links present in the network. The total number of links and nodes helps to comprehend the structure of the network i.e. whether the network is large or small. While examining the criminal network, the understanding of network is of crucial importance. For the sake of clarity, the robbery crimes are divided into different categories in table 3. The Crime characterization is based on crime types. Each crime type is assigned a distinct color and id. The color of each crime type is attached to the name of each criminal. This helps to have a quick understanding about the data of criminal and the type of crime he was involved in. For instance, if the criminal Kashif is involved in committing robbery crime of category1, the color assigned to category1 is visualized with the criminal name. One criminal can be involved in more than one crime and may be a part of one or any other group. That is why the names of the criminals are repeated in the network. This helps to understand the network in terms of viewing a criminal individually and also as a part of a group or subgroup. This gives the insight to examine the structure of the network closely and distinctly.

3.2 Network nodes and links

The network may have one to several nodes. The presence of a huge number of nodes complicates the network. Few nodes are standing individually in the network while others are merged in the form of groups. The nodes are connected to each other on the basis of robbery crime in which they were reportedly involved. The links among criminals are visualized using show link feature of PEVNET tool. The overall link information of the network is visualized. One node may have links to more than one criminal. To make the links more clear and visible, the blinking option proved to be very helpful. The links among criminals blink on clicking the desired node in the network. The links take the form of thick lines visualizing the links among different nodes of the network. The size of a node is dependent on its crime weight. The weight of the node is actually the involvement of that node in respective crimes. It helps to differentiate between high weight and low weight criminal nodes. This gives an analytical and deeper understanding of network nodes and their corresponding links. The information of every link related to robbery data is visualized each time the node is accessed in a network. When a link is accessed, the information related to that link is shown in criminal record window of PEVNET tool. This information includes the robbery crime type, gender, crime type id and color accompanied by group information and pie charts. When a specific crime type is selected, the nodes of that crime type take a form of clusters and visualized in such a way that the cluster exclusively arise from the actual network.

3.3 Mapping crime patterns

The robbery crime patterns can be mapped through network visualization. Crimes are mapped by analyzing the network with utmost care and caution. The numbers of criminals that are found committing the same type of crime frequently are categorized

Table 3: Detailed description of crime categories

Crime Categories	***Robbed Items***	***Category Id***	***Category Color***
Category1	Cash	1111	Yellow
Category2	Cash, jewelry, mobile	2222	Gold
Category3	Cash, mobile	3333	Turquoise
Category4	Cash, jewelry	4444	Blue
Category5	Jewelry, mobile	5555	Grey
Category6	Mobile	6666	Pink
Category7	Tower batteries	7777	Mustard

through network visualization. The network shows the repeated criminal nodes and their links with other groups and subgroups. The repeated criminals contribute to the seriousness of apprehending the intersecting nodes and complex links. The identification of reciprocating criminal links leads to the mapping of crime patterns. By mapping these links the hidden information is revealed and the central person can be located. There is also an existence of sequence in these robbery crimes. Most of the crimes in robbery dataset are committed by alternate groups
but few criminals occupy the central position in every group. The dataset also reveals that few groups commit the same type of robbery over and over again. Network visualization aids in analyzing the criminal mindset and locating central persons. It helps in mapping crime patterns, identifying repeating links and visualization of group information in the form of clusters.

3.4 Predicting future crimes

Crime prediction has always been a challenge for law enforcement agencies. Crimes can be predicted by

observing every minute criminal profiling detail. Using robbery crime dataset as an experimental basis, few observations are extracted by visualizing the detailed robbery data in PEVNET. PEVNET's trend analysis and similar node map feature are significant in this regard. The trend analysis feature shows the trends of reported robbery cases. The similar node map feature gives the geographical information about robbery crime locations. The trend analysis provides information about the high and the low crime trend rate in a network. The analysis of crime trend rates and the geographical information of repeated crime locations would be of greater help to predict crime. It would highlight most vulnerable crime types and identify crime-prone areas. This would greatly help legal bodies to prevent and predict robbery crimes.

4. Results and Discussion

Creative visualization of information related to robbery crimes provides a greater interpretation of network structure. The visualization of robbery crime dataset in Fig. 1 shows the overall pattern of network formation. The nodes are shown in the PEVNET visualization stage and the links among criminals are also depicted in Fig. 1. The robbery crimes types are also visualized in the network. Each crime type has an independent id and color. Crime types are categorized on the basis of essentials being robbed such as cash, cash and jewelry, cash jewelry and mobile phones, jewelry, cash mobile phones, and tower batteries. Each crime type is assigned to a unique id. The purpose of this division is to distinguish each crime type distinctly. Similarly, the information about the total estimated amount of robbed items is also incorporated into the data network visualization. This information is also available when the purpose is a thorough investigation of crimes. The communication link between criminals belonging to unassociated crime categories are also illustrated in the network. The names of all the criminals are shown with their respective crime category color. The crime categories are also visible on the right-hand side of the visualization stage. This whole set of information helps in apprehending the overall structure, scheme of nodes and links, identification of communication type i.e. whether the communication is one way or two-way process in the criminal network as shown in Fig. 1. Identifying the criminal links is made easy using PEVNET. By selecting a crime type e.g. cash category, the criminal link information related to that specific category is visualized. This information aids in developing an understanding of criminal links and link patterns separately as shown in Fig. 2.

Blinking of links thickens the interacting nodes in the network. Several linking nodes are shown distinctly and each node is connected to its corresponding root node. The addition of new nodes doesn't disturb the whole network. New nodes can be added and the previous nodes can be deleted with ease. The linking pattern shows how the nodes are connected and how many groups exist in the network is shown in Fig. 3. Mapping of crimes is done by charting out the criminals involved in different crime types. A single criminal who found involved in different robbery crime cases is sometimes the mastermind of such crimes. A close observation of criminal network leads to identify that central person and to map crime patterns by inspecting the previous group activities. For instance, criminals Ali and Wasim are involved in crime category1 and in crime category2 respectively as shown in Fig. 2-3. All the repeating nodes in the network are linked to each other in the same pattern. By examining the crime patterns, mutual links and their respective crime weight leads to an extended crime mapping.

The target of predicting robbery crimes is chased through the observation process. Observing and analyzing crime trends lead analysts to predict future crime. PEVNET gives detailed information about crime trends based on given dataset. A crime trend analysis based robbery crime dataset is shown in Fig. 4. The trend of each crime category is shown with colors assigned to each crime type in oval-shaped circles. In the same window of PEVNET tool, a graphical representation of the crime trend is also depicted. This information provides grounds for predicting crimes. Geographical information of crime locations is supportive when combined with trend analysis feature of PEVNET. By maintaining the record of the top criminals of every network is also a leading clue in the pursuit of predicting crimes. PEVENT keep track of repeated criminals of a network and rank them in a graph on the basis of their crime weight as shown in Fig. 5. Mostly the most powerful node in a network is basically the spermatozoa of the criminal network. On a graph, criminals are ranked on the basis of their crime involvement ratio. If a similar robbery case is reported in future, these criminals can be accessed by the investigative agencies as the prime suspects of the reported crime. The information of every node can separately be acquired using criminal record window. Facts and figures related to a single or group of nodes can be extracted from this window. Pie charts are generated for each criminal regardless of their crime involvement categories. In the pie charts, the crime category color occupies the central position as shown in Fig. 6. Crime weight of top criminal of the network belonging to category1 is represented in Fig 6

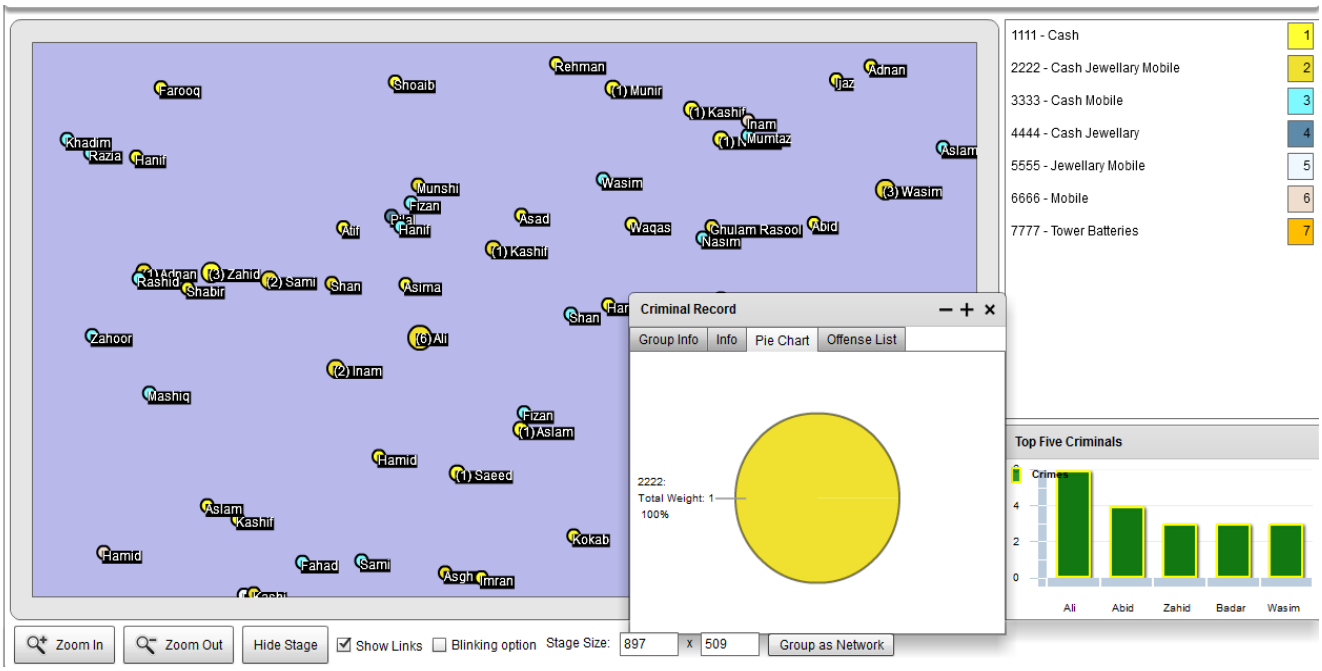

Fig. 1 The inclusive structure of the network

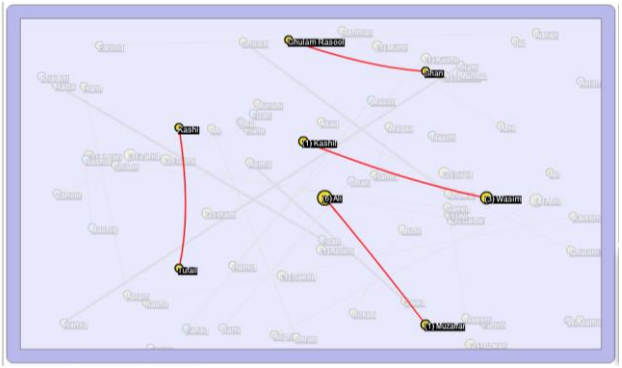

Fig. 2 The repeated criminals in the network

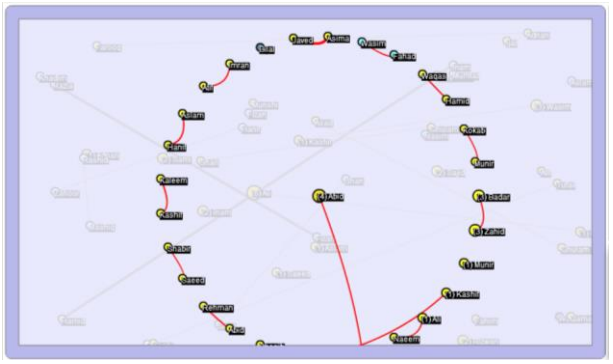

Fig. 3 The placement of nodes and pattern of linkage in the network

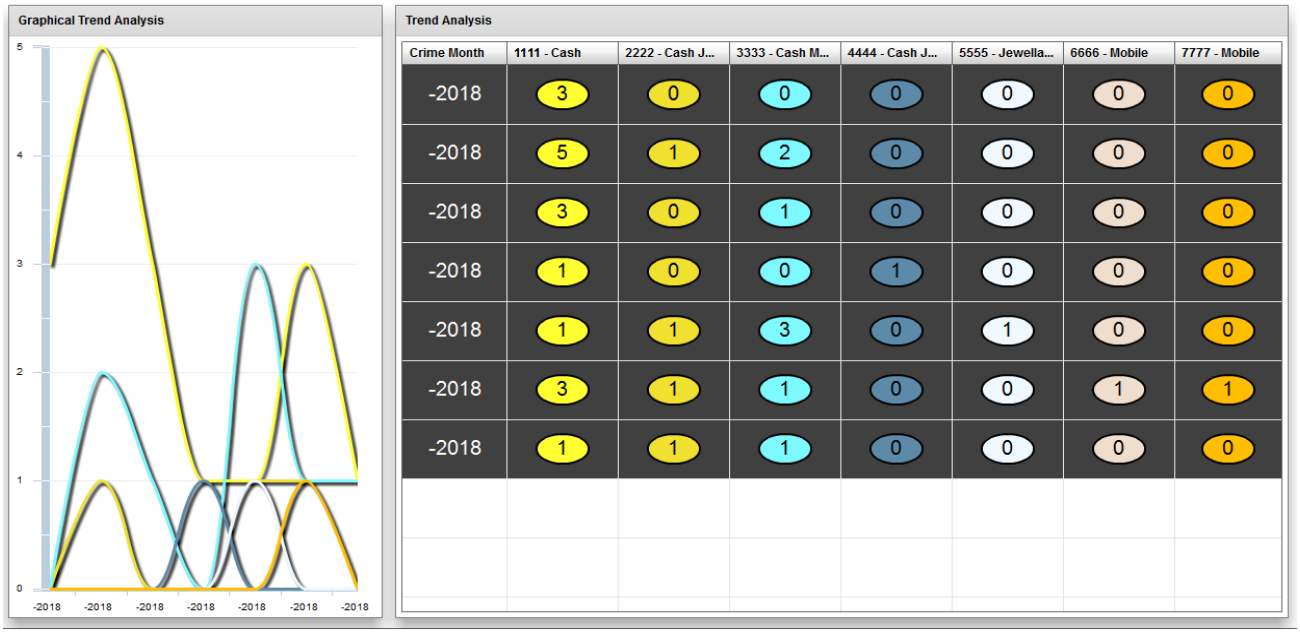

Fig. 4 Crime trend analysis

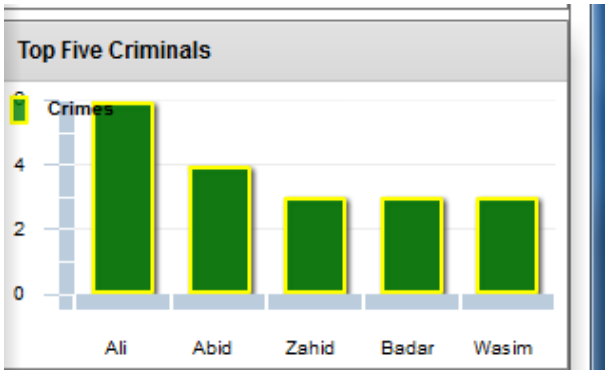

Fig. 5 Top five criminals of the network

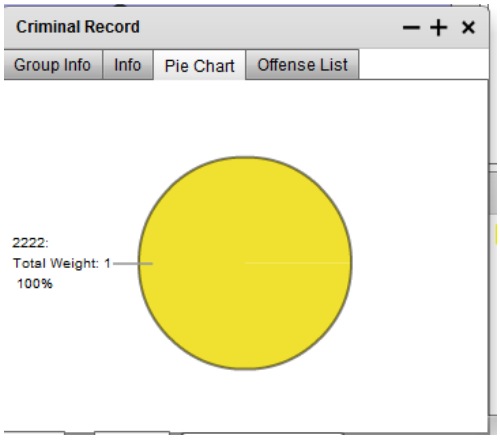

Fig. 6 Pie chart based on crime weight

5. Conclusion

In this research is attempted to understand the covert nature of temporal criminal network by carrying out network visualization and analysis. PEVNET is used to demonstrate the research and the experiment is performed on a real dataset. The complexity of criminal networks makes it difficult to predict their approximate future interventions. The mushroom growth of criminal networks has raised many concerns for the law enforcement bodies and the policymakers. The enhanced technological methods have also facilitated criminals in very negative terms. There is a dire need to strategically target the potential criminal networks by combining the legal and technological approaches to eradicate such criminal setups. Various machine learning techniques and visualization tools e.g. Gephi, Cytoscape, COPLINK, CrimeFighter, CrimeNet, Pajek, and Tulip have been applied earlier to overcome network visualization and analysis problem. But no tool provides a complete solution to such problems. PEVNET provide solutions to many visualization and analysis problems in competition with other states of the art tools.

References

[1] J. D. Haider, P. Seidler, M. Pohl, N. Kodagoda, R. Adderley, and B. L. W. Wong, “How Analysts Think : Sense-making Strategies in the Analysis of Temporal Evolution and Criminal Network Structures and Activities,” no. 2015, pp. 193–197, 2017.

[2] E. J. Castilla, "#2194-ASQ V50 N1-March 2005 — file: 50105-book-reviews," no. March, pp. 148–152, 2005.
[3] D. Bright, C. Greenhill, T. Britz, and A. Ritter, "Criminal network vulnerabilities and adaptations," Glob. Crime, vol. 00, no. 00, pp. 1–18, 2017.
[4] J. J. Xu and H. Chen, "CrimeNet Explorer : A Framework for Criminal Network Knowledge Discovery," vol. 23, no. 2, pp. 201–226, 2005.
[5] A. Rasheed and U. K. Wiil, "Evaluating Criminal Networks with PEVNET," Proc. 2015 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Min. 2015 - ASONAM '15, pp. 1028–1031, 2015.
[6] Y.-C. Chang, K.-T. Lai, S.-C. T. Chou, and M.-S. Chen, "Mining the Networks of Telecommunication Fraud Groups using Social Network Analysis," Proc. 2017 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Min. 2017 - ASONAM '17, pp. 1128–1131, 2017.
[7] A. Rasheed, "A Tool for Analysis and Visualization of Criminal Networks," pp. 97–102, 2015.
[8] P. P. Shah and R. Mehta, "Comparative Analysis of Social Network Analysis and Visualisation Tools," vol. 3, no. 1, pp. 508–513, 2017.
[9] A. Rasheed and U. K. Wiil, "A Tool for Analysis and Visualization of Criminal Networks," Proc. - UKSim-AMSS 17th Int. Conf. Comput. Model. Simulation, UKSim 2015, pp. 97–102, 2016.
[10] J. J. Xu and H. Chen, "Fighting organized crimes: Using shortest-path algorithms to identify associations in criminal networks," Decis. Support Syst., vol. 38, no. 3, pp. 473–487, 2004.
[11] B. Schröter et al., "Strengths and weaknesses of the Net-Map tool for participatory social network analysis in resource management: Experience from case studies conducted on four continents," Methodol. Innov., vol. May-August, pp. 1–7, 2018.
[12] J. Schroeder, "COPLINK : Database Integration and Access for a Law Enforcement Intranet," p. 132, 2001.
[13] H. Maps, "The Mantra of Visual Information Seeking The Pursuit of Insights," 2010.
[14] N. Alcaraz et al., "KeyPathwayMiner 4.0: Condition-specific pathway analysis by combining multiple omics studies and networks with Cytoscape," BMC Syst. Biol., vol. 8, no. 1, pp. 1–6, 2014.
[15] U. K. Wiil, N. Memon, and J. Gniadek, "CrimeFighter: A toolbox for counterterrorism," Commun. Comput. Inf. Sci., vol. 128 CCIS, pp. 337–350, 2011.
[16] R. R. Petersen and U. K. Wiil, "CrimeFighter investigator: A novel tool for criminal network investigation," Proc. - 2011 Eur. Intell. Secur. Informatics Conf. EISIC 2011, pp. 197–202, 2011.
[17] U. K. Wiil, J. Gniadek, N. Memon, and R. R. Petersen, "Knowledge management tools for terrorist network analysis," vol. 272 CCIS, pp. 322–337, 2013.
[18] D. Auber, "Tulip — A Huge Graph Visualization Framework," pp. 105–126, 2004.
[19] G. A. Pavlopoulos, D. Malliarakis, N. Papanikolaou, T. Theodosiou, A. J. Enright, and I. Iliopoulos, "Visualizing genome and systems biology: Technologies, tools, implementation techniques and trends, past, present and future," Gigascience, vol. 4, no. 1, 2015.
[20] A. Mrvar and V. Batagelj, "Analysis and visualization of large networks with program package Pajek," Complex Adapt. Syst. Model., vol. 4, no. 1, 2016.