ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(31), DOI:10.17485/ijst/2015/v8i31/75197, November 2015* ISSN (Online) : 0974-5645

A Survey on Different Graph Based Anomaly Detection Techniques

Debajit Sensarma* **and Samar Sen Sarma***

Department of Computer Science & Engineering, University of Calcutta, Kolkata - 700073, West Bengal, India; debajit.sensarma2008@gmail.com, sssarma2001@yahoo.com

Abstract

This survey paper cites some methods of graph based anomaly detection in the field of information security, finance, cyber-security, online social networks, health care, law enforcement etc. and their classification. Finally, the relevance of cyber crime and its elimination is highlighted throughout the paper with some real world applications of graph based anomaly detection techniques and also some future direction to improve the technique of detecting anomalies in data has been given.

Keywords: Anomaly Detection, Fraud Detection, Graph, Online Social Networks, Outlier Detection, Security

1. Introduction

In the broad area of applications such as fraud detection for online social networks, telecommunication, credit cards, insurance or health care, intrusion detection for cyber-security, fault detection in safety critical systems etc., anomaly detection comes to the scene[1,2].The main problem is to find patterns in data that do not abide by the expected behavior. These abnormal patterns are often referred to as anomalies, outliers, exceptions, and aberrations etc., which are different in different application domains.It is a very challenging task because now-a-days the size of the network data are very large and also increasing day by day.Numerous researches have been going on in diverse areas and application domains to cope with this problem.While working with this large scale data, interconnection between the entities often provides additional information that may be exploited for detection of anomalous events efficiently. This type of interconnectivity and inter relation between the data can be efficiently modeled using graph. In various application domains proper anomaly detection can tells when and what actions should be taken to prevent loss. For example, by investigating an anomalous traffic pattern in a computer network it can be said that sensitive data are sending out by a hacked computer to an unauthorized destination. Again, when an MRI image is anomalous then it may indicate presence of malignant tumors. Besides this, in credit card transaction, data anomalies could indicate credit card theft. In the statistics community, detecting anomalies in data has been studied extensively as early as the 19th century[3].

As graph data becoming ubiquitous now-a-days, the techniques for structured graph data have been in limelight recently. Many works have been developed in the field of anomaly detection using graph data, as objects in graphs have long-range correlations. So, graph can be used as unified frameworks for solving anomaly detection problems in several application domains.

In this work, anomaly detection methods for detecting anomalous data where data represented as graphs are depicted in a nutshell and it contains a short review of recent existing graph based anomaly detection methods and its outcomes. Also some real world applications

* *Author for correspondence*

of graph based anomaly detection methods have been given with future directions to improve the approach of detecting anomalies in data in short.

The paper is organized as follows: Section 2 describes challenges associated with anomaly detection problem. Section 3 describes the advantages of using graph data for anomaly detection. In section 4 various existing graph anomaly detection methods are described in brief. Section 5 gives the applications of graph based anomaly detection in various real world application domains. Finally section 6 concludes the paper giving some future scopes.

2. Challenges in the Field of Anomaly Detection

An anomaly is defined as a pattern that does not conform to expected normal behavior in an abstract sense. Therefore in a straightforward way the aim of the anomaly detection approach is to define a region that represents normal behavior and area in the data which does not belong to this normal region treated as anomaly. But there are several factors that make this approach very challenging:

- Defining a normal region with all possible normal behavior is very difficult. Because the boundary between normal and anomalous behavior is often not precise. So, an anomalous observation which lies closely with the boundary of normal observations can actually be normal, and vice-versa.
- Normal behavior keeps evolving in various domains and a current notion of normal behavior might change completely in the future.
- The actual notion of an anomaly is different for different application domains, e.g. deviation in stock price in the stock market domain is considered as normal where in the medical domain a small deviation in body temperature from normal might be an anomaly. Thus anomaly detection technique developed for one domain is not applicable for another domain.
- In most of the cases the task of differentiating normal behavior is more difficult because of malicious adversaries often adapt themselves after some malicious actions and make the anomalous observations appear like normal.
- Noisy data often behaves like the actual anomalies and so they are also difficult to distinguish and remove.

Due to the above challenges it is not very easy to solve the anomaly detection problem. Most of the existing anomaly detection techniques solve the problem by formalizing the problem considering nature of the data, availability of labeled data, and type of anomalies to be detected, etc.

3. Advantages of Graphs in the Field of Anomaly Detection

Here we give four reasons of how graph is advantageous for anomaly detection.

- Most of the data objects are often related to each other and there are some dependencies. Majority of the relational data can be thought of as inter-dependent, which may help to find anomalies in large interconnected networks. For example biological data such as the food web and Protein–Protein Interaction (PPI) networks, terrorist networks, email and phone-call networks, retail networks, blog networks, social networks, to name but a few such networks that possess high cohesiveness[2] .
- Problems in anomaly detection domain are mostly relational in nature. The nature of anomalies could exhibit themselves as relational. For example in the fraud domain, the fraudsters are most of the cases related or interconnected to each other. These phenomena can be easily and efficiently modeled as graph.
- Graph has a powerful representation which is used to represent inter-dependencies by the introduction of links (or edges) between the related objects very efficiently. The long-range correlations can be measured using the multiple paths lying between these related objects. Furthermore, representation of rich datasets is permit-ted by the graphical representation which enables the incorporation of node and edge attributes.
- Adversarial robustness, which is very important is provided by graph e.g. in fraud detection systems, behavioral clues such as log-in times and locations (e.g., IP addresses) can easily be altered by advanced fraudsters. Besides this, it may be reasonable to argue that the fraudsters could not have a global view of the entire operating network (e.g., money transfer, telecommunication etc.). In that case it would be harder for a fraudster to fit into this network properly without knowing its entire characteristic structure and dynamic operations.

4. Existing Graph Based Anomaly Detection Methods

In this section the existing works on graph anomaly detection techniques are described by dividing them into two categories namely static graph anomaly detection,

dynamic graph anomaly detection (depicted pictorially in Figure 1.).

4.1 Static Graph Anomaly Detection

This section deals with finding anomalous entities (e.g. nodes, edges, sub-graphs) in static snapshot of graph.

4.1.1. Structure Based Anomaly Detection

There are mainly two types of structure based anomaly detection techniques namely anomalies in static plain graphs and anomalies in static attributed graph. They are described below.

Firstly, in anomaly detection scheme in static plain graph, various graph centric features like node degree, centrality, egonet etc. are extracted and a feature space is constructed taking together with other features extracted from additional information sources for anomaly detection. Hassanzadeh et al proposed[4] an anomaly detection technique where they use graph metrics for identifying users with anomalous relationships to other user in online social networks. They have used various graph theoretic properties such as- number of neighboring nodes and edges, betweenness centrality and community cohesiveness for differentiating people's online behavior by their usage pattern. Normal users follow common patterns whereas abnormal users do not follow the normal behaviour. Besides this, looking at the relationships of users can reveal meaningful patterns because user can hide their identity by providing false information but cannot hide links that they have established with others. They use local metrics like- single node (ego), 1-level neighborhood (an egonet), 2-level neighborhood (a super egonet) and betweenness centrality and average betweenness user's egonet, community cohesiveness of user's super egonet are measured for identifying users with anomalous link structures. They also evaluated the method with the existing data collected from three online social networks (Facebook, Orkut, Flickr) and concluded that in particular average betweenness centrality gives better accuracy in detecting anomalies than existing approaches.

In case of static attributed graphs, the main goal is to identify substructures in the graph that are rare structurally with respect to both the connectivity-wise, as well as attribute-wise. Mookiah et al proposed a graph based anomaly detection method called GBAD[5]. It is basically based upon the theory that a person attempting to commit an unusual or illegal action would do so by imitating the known behaviors thus concealing their true intensions. It mainly consists of three different algorithms- GBAD-MDL, GBAD-MPL and GBAD-P. GBAD-MDL algorithm finds the normative substructure using Maximum Description Length principle (MDL) and further finds similar substructures with acceptable level of modification from normative sub-structure. GBAD-MPL algorithm also determines the best substructure by looking at edges and vertices that are missing .The GBAD-P algorithm uses the MDL evaluation technique to discover the best substructure in a graph, but instead of examining all instances for similarity, this approach examines all extensions to the normative sub-structure (pattern), looking for extensions with the lowest probability. The authors used this method to discover suspicious employees and their actions as a tool for supporting potential criminal investigation.

4.1.2 Community based Anomaly Detection

The aim of this technique is to find the densely connected nodes in the graph that forms cluster and spot the node that have inter cluster connectivity.

Moradi et al proposed a community based anomaly detection method[6] by identifying communities that do not respect the community boundaries. This work is based on a hypothesis that misbehaving nodes tend to belong to multiple communities. To achieve this, authors enhanced disjoint communities where each node only belongs to a single community, with a layer of auxiliary communities. This community is formed over the boundaries of neighboring communities which allows a node to be the member of several communities and this enhancement can be used to identify anomalies in network traffic. They also applied this method to identify network intrusion and unsolicited emails in two different datasets generated from network traffic collected on a 10 Gbps Internet backbone link of a large national university network and they have shown that, this method is very effective and provides consistent performance over time.

Perozzi et al proposed a method[7] called focused clustering and outlier detection in static attributed graphs namely FocusCO. The algorithm mainly has three steps. (i) Inferring attribute weights (ii) extracting focused clusters and (iii) outlier detection. In short, the aim is to output a set of nodes provided by a user those are agreed upon the 'focus attributes'. In this method, a

cluster of densely connected nodes called 'focus clusters' are found with respect to the 'focus attributes' and based on the focused clusters an outlier is defined as a node that structurally belongs to the cluster but deviates much in focus attributes. They have shown that the method is very effective and scalable for synthetic and real world graphs. Also it outperforms various existing algorithms.

4.2. Dynamic-Graph Anomaly Detection

Real world graphs are constantly evolving. Detecting anomalies in this type of dynamic graphs are very challenging task. Here, mainly 6 methods for dynamic graph anomaly detection have been considered.

4.2.1. Distance Based Anomaly Detection

Distance based metric can be used to measure the change between two objects. Two objects having a small difference in measured metric are said to be similar. There are various metrics for detecting anomalies, e.g. Error correcting graph matching distance, Maximum Common Sub graph (MCS) distance of adjacency matrices, Graph Edit Distance (GED), Hamming distance for the adjacency matrices of the graphs etc. Gaston et al. proposed a way[8] to detect abnormal changes in time-evolving communication graphs using diameter distance which is measured by difference in graph diameter (i.e. greatest of the longest shortest path of all vertices).

4.2.2. Compression based Anomaly Detection

In this process a compact graph representation is achieved using Minimum Description Length (MDL) and compression technique by exploiting patterns and regularities of data with minimum encoding cost. Anomalies then defined as graphs that prohibit compression. The Sun et al proposed an algorithm[9] called GraphScope which is an MDS based, parameter free algorithm for discovering node partition in streaming graphs and monitoring their evolution over the time in order to detect abnormal events.

4.2.3. Decomposition Based Anomaly Detection

This method detects temporal anomalies by representing set of time evolving graphs as a tensor or multidimensional array and performing factorization or dimensionality reduction. Sun et al proposed a novel method[10] called Compact Matrix Decomposition (CMD), to compute sparse low rank approximations. The reconstruction error of each sparse graph is tracked over time and if it changes much at some time, the corresponding graph is anomalous.

4.2.4. Community or Cluster Based Anomaly Detection

In case of community or cluster based method, instead of monitoring changes in whole network, a community is being monitored over time for any anomalous events. Aggarwal et al. provide a structural outlier detection scheme[11] in massive network streams by dynamically partitioning the network in order to construct statistically robust models of connectivity behavior.

4.2.5. Probabilistic Model Based Anomaly Detection

The probability theory construct model which can be treated as normal and deviation from this model are marked as anomalous. A two stage method[12] has been pro-posed by Heard et al. where first stage consists of simple, conjugate Bayesian models for discrete time counting processes to track the pair wise links of all nodes in the graph for assessing normality behaviour and standard network inference on greatly reduced subset of potentially anomalous nodes is applied in second stage.

4.2.6. Window Based Anomaly Detection

Anomaly detection algorithms provide some methods which are bound to a time window in order to detect anomalies. Eberle et al[13] proposed an approach called Pattern Learning and Anomaly Detection on Streams (PLADS), which is a partitioning and windowing approach that partitions the graph as it streams in over time and maintains anomalies and normative patterns which is biased towards the set of normative patterns found in the 'current time window'. It is also scalable to real world data and also very effective in detecting anomalies.

5. Applications of Graph Based Anomaly Detection

Some real world applications of graph based anomaly detection techniques have been given below in Table 1.

Table 1. Applications of Graph based Anomaly Detection Techniques

Anomaly Detection Schemes	Type of Anomaly Detects	Methodology	Results
Detecting Anomalies in Mobile TelecommunicationNetworks Using a Graph Based Approach [14]	Mobile Telecommunication Fraud	Telecom data (phone call and message data) are represented as a graph and Graph-Based Anomaly Detection (GBAD) tool[5] is used to find anomaly in the data.	Authors have used anonymized cellular phone data provided by Nokia through the 2012 Mobile Data Challenge (MDC) as data set. They claimed that it can prove beneficial to emphasize on graph based representation of data for detecting anomalies in Mobile Telecommunication Networks and with the real world data the graph representation allows detection of 5 (but 3 unique) anomalous substructure in mobile call graph, two of which are detected using distinct evaluation metrics with different normative patterns.
Using Neighbor Diversity to Detect Fraudsters in Online Auctions[15]	Online Auction Fraud	Approach is based on neighbor diversity of each trader for detecting fraudsters. The intuition is that the neighbor of a fraudster is likely to have similar patterns and have a low diversity. Four types of neighbor diversity based on number of received ratings, the number of cancelled transactions, the joined date and k-core have been proposed.	Performance of the algorithm are evaluated using real world dataset collected from Ruten (www.ruten.com.tw), which is one of the largest auction websites in Taiwan. The neighbor diversity on the number of received ratings or on the number of cancelled transactions significantly improves the performance; recall and F_1-measure sometimes reduce the precision. However the result on neighbor diversity based on k-core or on the joined data shows little or no improvement.
Guilt-by-Constellation: Fraud Detection by Suspicious Clique Memberships[16]	Social security fraud	Introduced a clique-based features which are used to detect fraudulent companies in three steps- (i) Propagating a time-dependent exposure score for each node based on its relationships to known fraud in the network. (ii) Deriving cliques of companies, resources and labeling cliques in term of fraud and involvement in bankruptcy. (iii) Characterizing each company using combination of intrinsic and relational features and its membership in suspicious cliques.	For each timestamp approximately 220,000 active companies and 5 million resources are registered with social security institution has been taken as dataset. Performance has been measured with respect over time, precision and variable importance and this method is able to uncover 22% fraud cases.
A New Clustering Approach For Anomaly Intrusion Detection[17]	Network intrusion detection	Approach is based on medoid clustering algorithm and certain modifications of it. It is better than k-means algorithm and overcomes the disadvantages of dependency on initial centroid, number of clusters and irrelevant clusters.	KDD cup99 data set (first given by Massachusetts Institute of Technology for intrusion detection) is used for the experiment. The accuracy of the algorithm is 96.38% which is comparatively higher than the existing k-means, FCM and Y-means algorithms.
Review graph based online store review spammer detection[18]	Anomalies in opinion networks	Heterogeneous review graph concept is used to capture the relationship among reviewers, review and stores that the reviewers have reviewed. This type of interaction between nodes can reveal the cause of spam and also the suspicious reviewers can be identified.	Store review data from www.resellerratings.com, which is a largest host of review stores, has been used for the experiment. This method can identify delicate spamming activities with good precision (according to the experiment, 49 out of 100 suspicious candidates are spammers, i.e. precision 49%) and human evaluator agreement.

Abnormal Web Traffic Detection Using Connection Graph[19]	Web Traffic anomaly	In this method, web requests are extracted from web or proxy server which is great source of knowledge about usage pattern of different clients. Two features are used to filter out the suspicious clients generating abnormal traffics namely- (1) malicious server degree (MSD) which evaluates how much the server is malicious and (2) abnormal traffic scores (ATS) which points out possible clients who can generate suspicious traffic.	File of web log data are collected from proxy server in 1 day worth, on Monday 01 October 2012, of web traffic in a large university environment serving a total user population in excess of 2000 clients, and accounted for over 4.2 million records (847 MB). Analyzed data is extracted within 2 hours from 08:00 AM to 10:00 AM which is in working time and people accessed the Internet very much. Experiment shows that it is a very effective method for large network and detected abnormal web traffic is easy to be visually seen.

6. Conclusion and Future Scopes

The aim is not to claim the superiority of graph-based methods over other detection techniques, rather to covey the expressiveness of graphs in capturing real world phenomena, which makes them very powerful machinery for abnormality detection. Mainly three issues are emphasized; (1) data instances are often interdependent and exhibit long-range correlations, (2) the anomaly detection problem is often relational in nature (e.g., opportunistic or organized fraud), and (3) robust mechanism is necessary to fight with the attackers (e.g. in fraud scenarios). Graphs prove to be effective in all these aspects. After studying some existing works some future scopes can be inferred.

- Anomaly Prevention is very necessary to save the criminal activities. For this it is very much needed to detect anomaly in real time and before actually it can happens. Although some works[16,20] exits but still lots of improvements required.
- Graph Theoretic codes are majority decodable[21]. It can be used for error correction and detection. The circuit matrix (or cut-set matrix) of a linear graph 'G' is a binary linear code of distance 'd' and length n-an (n, d) code; where n is the number of branches in G and d is minimum number of branches in a circuit (or a cut-set) of G. In future, it can be used to track abnormalities in the graph structure and can be used to differentiate between normal and abnormal patterns.
- Many algorithms for time-evolving graphs require a time-window for feature extraction or computation of the normal graph/node activity; one of the open questions is how to choose this window in order to discover the different types of outliers in the graph sequences is still open.
- Most methods in the data mining and machine learning community focus on detection performance while ignoring adversarial robustness. It is of high interest, from the practitioner's point of view, to understand the adversarial robustness of a new algorithm; i.e. how easy it is to break the algorithm or what is the minimum amount of knowledge or computational power the attacker needs to have access to, in order to disguise their bad activities.
- Most methods ignore the cost aspects of information. These costs, on the other hand, may exhibit themselves in various forms with varying levels, e.g., cost in measurement and monitoring applied on the system; cost in being exposed to certain types of attacks exerted on the users; and cost in getting around of the algorithms exerted on the adversaries (which also relates to the above). These varying costs should be accounted for differently in algorithm development.
- Last but not the least; it may be the case that there is more than one network available, capturing different aspects of relations (e.g., friendship network among the same individuals). While possibly beneficial, how to exploit all available networks and fuse clues from all these sources for anomaly detection remains an open area.

7. Acknowledgment

The authors would like to thank UniversityOf Calcutta, West Bengal, India, Department of Science & Technology (DST), New Delhi, for financial support and the reviewers for their constructive and helpful comments and specially the Computer without which no work was possible.

8. References

1. Oxford English Dictionary. Oxford: Oxford University Press. 1989.

2. Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey. Data Mining and Knowledge Discovery. 2014; 29(3): 626-88.
3. Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM Computing Surveys (CSUR). 2009; 41(3):1-15.
4. Hassanzadeh R, Nayak R, Stebila D. Analyzing the effectiveness of graph metrics for anomaly detection in online social networks. In: Web Information systems Engineering-WIsE 2012. Springer Berlin Heidelberg. 2012; 7651: p. 624-30.
5. Mookiah L, Eberle W, Holder L. Detecting suspicious behavior using a graph-based approach. In: Visual Analytics Science and Technology (VAST). IEEE. Paris, France. 2014: p. 357-58.
6. Moradi F, Olovsson T, Tsigas P. Overlapping Communities for Identifying Misbehavior in Network Communications. In: Advances in Knowledge Discovery and Data Mining. Springer International Publishing. Taiwan. 2014; 8443: 398-409.
7. Perozzi B, Akoglu L, Sánchez IP, Müller E. Focused clustering and outlier detection in large attributed graphs. In: Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining. USA. 2014: p. 1346-55.
8. Gaston ME, Kraetzl M, Wallis WD. Using graph diameter for change detection in dynamic networks. Australasian Journal of Combinatorics. 2006; 35:299-311.
9. Sun J, Faloutsos C, Papadimitriou S, Yu PS. Graphscope: parameter-free mining of large time-evolving graphs. In: Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM. USA. 2007: p. 687-96.
10. Sun J, Xie Y, Zhang H, Faloutsos C. Less is more: Sparse graph mining with compact matrix decomposition. Statistical Analysis and Data Mining: The ASA Data Science Journal. 2008; 1(1):6-22.
11. Aggarwal CC, Zhao Y, Yu PS. Outlier detection in graph streams. In: Data Engineering (ICDE). 2011 IEEE 27th International Conference on IEEE. Hannover. 2011; p. 399-409.
12. Heard NA, Weston DJ, Platanioti KH and D J. Bayesian anomaly detection methods for social networks. The Annals of Applied Statistics. 2010; 4(2): 645-62.
13. Eberle W, Holder L. A partitioning approach to scaling anomaly detection in graph streams. Big Data (Big Data), 2014. IEEE International Conference. IEEE. Washington DC. 2014; p. 17-24.
14. Chaparro C, Eberle W. Detecting Anomalies in Mobile Telecommunication Networks Using a Graph Based Approach. The Twenty-Eighth International Flairs Con-ference. Florida. 2015: p. 410-5.
15. Lin JL, Khomnotai L. Using Neighbor Diversity to Detect Fraudsters in On-line Auctions. Entropy. 2014; 16(5): 2629-41.
16. Vlasselaer VV, Van Vlasselaer V, Akoglu L, Eliassi-Rad T, Snoeck M, Baesens B. Guilt-by-Constellation: Fraud Detection by Suspicious Clique Memberships. In: Proceedings of 48 Annual Hawaii International Conference on System Sciences. Kauai, HI . 2015: p. 918-27.
17. Ranjan R, Sahoo G. A New Clustering Approach For Anomaly Intrusion Detection. arXiv preprint arXiv:1404.2772. 2014:p. 29-38.
18. Wang G, Xie S, Liu B, Yu PS. Review graph based online store review spammer detection. In: Data Mining (ICDM) 2011. IEEE 11th International Conference on. IEEE. Vancouver, BC. 2011: p. 1242-7.
19. Tran MC, Heejeong L, Nakamura Y. Abnormal Web Traffic Detection Using Connection Graph. Bulletin of Networking, Computing, Systems, and Software. 2014; 3(1): 57-62.
20. Kirchner C. Implementing social network analysis for fraud prevention. CGI Group Ind. 2011.
21. Hakimi SL, Bredeson JG. Graph theoretic error-correcting codes. IEEE Transactions on Information Theory. 1968; 14(4): 584-91.
22. Javidi MM, Rafsanjani MK, Hashemi S, Sohrabi M. An overview of anomaly based database intrusion detection systems. Indian Journal of Science and Technology. 2012 Oct; 5(10): 3550-9.
23. Renjit JA, Shunmuganathan KL. Network based anomaly intrusion detection system using SVM. Indian Journal of Science and Technology. 2011; 4(9): 1105-8.
24. Prakash A, Chandrasekar C. An Optimized Multiple Semi-Hidden Markov Model for Credit Card Fraud Detection. Indian Journal of Science and Technology. 2015; 8(2): 165-71.
25. Sherly KK, Nedunchezhian R. A Improved Incremental and Interactive Frequent Pattern Mining Techniques for Market Basket Analysis and Fraud Detection in Distributed and Parallel Systems. Indian Journal of Science and Technology. 2015; 8(18): 1-11.
26. Sapienza A, Panisson A, Wu J, Gauvin L, Cattuto C. Anomaly Detection in Temporal Graph Data: An Iterative Tensor Decomposition and Masking Approach. Proceedings of AALTD. Portugal. 2015: p. 117.
27. Beutel A, Akoglu L, Faloutsos C. Fraud Detection through Graph-Based User Behavior Modeling. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Colorado, US. 2015 Oc: p. 1696-7.
28. Mookiah L, Eberle W, Holder L. Discovering Suspicious Behavior Using Graph-Based Approach. In: The Twenty-Eighth International Flairs Conference Florida. 2015 Jun: p. 428-33.
29. Bridges RA, Collins JP, Ferragut EM, Laska JA, Sullivan BD. Multi-Level Anomaly Detection on Time-Varying Graph Data. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Paris, France. 2015.
30. Sahu MK, Ahirwar M, Shukla PK. Improved Malware Detection Technique Using Ensemble Based Classifier and Graph Theory. In: Computational Intelligence & Communication Technology (CICT). IEEE International Conference. 2015 Feb: p. 150-4.
31. Mishne G, Talmon R, Cohen I. Graph-Based Supervised Automatic Target Detection. Geoscience and Remote Sensing. IEEE Transactions on. 2015; 53(5): 2738-54.