Detection of Fake Accounts in Social Network

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Computer Science and Engineering

Submitted By

Sushil Kumar

(Roll No. 801332029)

Under the supervision of:

Mr. Ravinder Kumar
Assistant Professor

Mr. Raj Kumar Tekchandani
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Detection of Fake Accounts in Social Network"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Mr. Ravinder Kumar and Mr .Raj Kumar Tekchandani* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Sushil Kumar

Signature:

(Sushil Kumar)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Mr. Ravinder Kumar)
Assistant Professor
Computer Science and
Engineering Department

(Mr. Rajkumar Tekchandani)
Assistant Professor
Computer Science and
Engineering Department

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

The successful completion of any task would be incomplete without acknowledging the people who made it possible and whose constant guidance and encouragement secured the success.

First of all I wish to acknowledge the benevolence of omnipotent God who gave me strength and courage to overcome all obstacles and showed me the silver lining in the dark clouds. With the profound sense of gratitude and heartiest regard, I express my sincere feelings of indebtedness to my guides **Mr. Ravinder Kumar**, Assistant Professor and Mr. **Raj Kumar Tekchandani**, Assistant Professor, Computer Science and Engineering Department, Thapar University for her positive attitude, excellent guidance, constant encouragement, keen interest, invaluable cooperation, generous attitude and above all her blessings. They have been a source of inspiration for me.

I am also thankful to **Dr. Deepak Garg**, Head of Department, CSED and **Dr. Ashutosh Mishra**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I will be failing in my duty if I do not express my gratitude to Dr. S. S. Bhatia, Senior Professor and Dean of Academics Affairs in the University, for making provisions of infrastructure such as library facilities, computer labs equipped with internet facility, immensely useful for the learners to equip themselves with latest in the field.

Last but not the least I would like to express my heartfelt thanks to my parents and my friends who with their thought provoking views, veracity and whole hearted cooperation helped me in doing this thesis.

Sushil Kumar

Sushil Kumar

(801332029)

Abstract

Social network is the basic platform of today's world to get connected with the people having same type of interest, perform similar activities or known to each other. Being on network, there is always a chance of getting data hacked by some fraudster. As the users are unaware of the attacker, they simply share their information over the network. The fraudster enters into the network after detecting the weaker node of the network that has maximum information on its node as compared to other weaker nodes and tries to create a link with that node. Once the fraudster enters into the network, he tries to build trust so that it can gain access to the information present over the network. Social network is not just Facebook or LinkedIn or twitter but it goes far beyond that, all kinds of transactional data where two objects are related to each other implicitly or explicitly falls under a network. We propose an algorithm which creates a label on every node based on their behaviour in the network whether it is genuine or fake account. In this we measure the strength of every node in the network and compared it with the trust score calculated for every node. Based on these two parameters we classify the nodes into their respective class. Once each node has labels according to their behaviour, it is easier for the user to detect whether to accept the friend request from such a node or ignore it.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

Anomalies are the unexpected behaviour which leads to irregular and strange activities over a network. Anomaly detection is the technique of detecting these unexpected changes over a network by monitoring the network. As the tremendous growth in social network, the possibility of fraud is also increasing. Being a huge social network, it is a tedious job to analyze the whole network and find out the suspicious node. Social network provide a basic platform for persons who want to exchange their views over a network. As the friends on social network authenticate and verify each other, these persons become unconcerned about the potential threats that come through messages/ accepting unknown friend requests/e-mail. When these cases arise, network security plays a major role to prevent them from fraudulent nodes. .For an example to download all the profiles from Facebook which are more than 750 million with an average speed of 10 profiles per second, would take more than 2 years. There are some primary characteristics of social network like low entry barrier, huge number of friends, open platform and anonymity. These properties makes user comfortable as it provide an ease to explore the ideas with others but also leads social network vulnerable to the fraudsters. The detection of anomalies in online social network in comprised of two stages: the selection and calculation of network attributes and the classification of results from this feature space [1]. To combat fraud by analyzing the social data have certain limitations: limited data which is publicly available for performing certain analysis which can be used to detect the fraud in future and lack of efficient methods to detect suspicious activities like fake identity, online auction fraud. Fraudsters can be categorised into two sub-types i.e. internal fraudster and external fraudster [2]. Internal fraudster is the one from within the network whereas external fraudster may be criminal background, average offender and organised professional offender. For combating fraud, there are different kind of technologies contributed by Statistics and machine learning in the area of money laundering, e-commerce, intrusion detection and telecommunication [3].

1.1Social Network Analysis

Social Network Analysis (SNA) is a way of finding out connection and flow between individuals, groups, organizations and other entities. SNA is not about just Facebook

or Linked in or twitter but it goes far beyond that, all sort of transactional data where different entities are related to each other implicitly or explicitly falls under a network. Explicit links are like persons interacting to each other or persons exchanging money with each other and implicit links are links persons reviewing the same product on a particular website. The major characteristics of social network are:

1. There are huge collections of participants that participate in the network.
2. There is at least one link between entities present in the network. In Facebook or Google+, these links are denoted as friends.
3. Relationships in social network tend to form clusters. If node X is related to Y and Z, then the probability of having relationship between Y and Z is higher.

1.2 Graphical Representation of Social Network

For better understanding of social network, graphical representation is required. The persons or entities are represented by nodes or vertices and the relationship between these persons is represented by edges in the network. Mostly, the graph of social network is undirected as in the case of friend graph but it can be directed as in the case of Twitter.

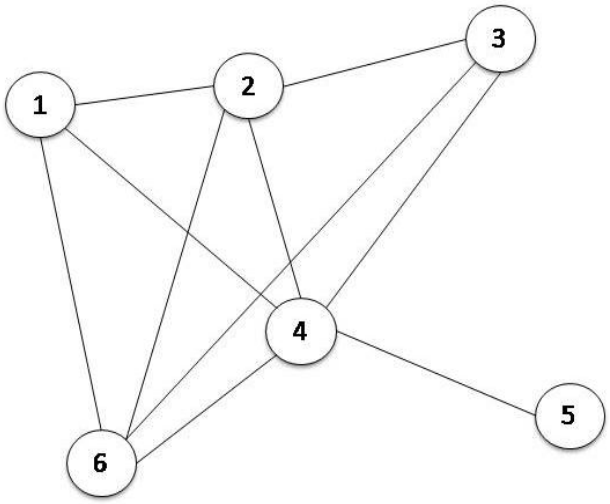

Figure 1.1 Graphical representation of a social network

In figure 1.1 a small network is represented. The individuals are represented by nodes from 1 to 6. The relationship between these nodes which might be a friend or follower relation is represented by the edges. For instance, node 3 is friends with node 2, 4, and

6. A *path* of the network is the collection of nodes which are connected by a link or edge.

- **Density**

It is the basic level of linking nodes in the social network. It is the ratio of the number of edges in a portion of a network to the maximum number of edges or links in a social network [4]. To calculate density,

$$Density = \frac{E}{n(n-1)/2}$$

Where E is the total number of observed edges and n is the total number of nodes in the network. n(n-1) calculates the maximum possible number of edges.

The value of Density may vary in the range [0,1], having 0 as the least density and 1 having maximum density. To detect potential fraud hotspots in retail sector density measure is extremely helpful.

- **Degree**

The total number of links of a node over a network is called the degree of that particular node. The degree can be classified in two types i.e. In-degree and Out-degree. In-degree is the total number on edges reaching that node in a directed graph and Out-degree is the total number of edges leaving that node. Commonly, in a social network an undirected graph is considered. A node with higher value of degree has higher influence as compared to other nodes in the network.

- **Closeness**

It gives the overall closeness of a node to every other node in the network. It is the inverse if farness to every node. It helps in accessing every other node fastest in the network [5].

- **Betweenness**

It is the measure of vertex in a graph which counts the number of nodes acting bridge when the shortest path between two other nodes. To calculate Betweenness in a graph G having vertices V and edges E, calculate the shortest path between each pair of vertices. Now, for each pair of vertices, find out the fraction of shortest paths which pass from the particular vertex. Calculate the sum of this fraction over each pair.

$$Betweenness = \sum_{x \neq v \neq y} \frac{\sigma_{xy}(v)}{\sigma_{xy}}$$

Where σ_{xy} is the total number of shortest paths from node x to node y and $\sigma_{xy}(v)$ is the number of paths passing through vertex v.

Centrality of a network can be calculated by degree, closeness and betweenness in the network. The concept of centrality was first explored in social network analysis. It gives the most influential node of the graph by calculating all the factors.

- **Structural holes**

Structural hole in a network occurs when a node from cluster A having link with other clusters so that none of other node from cluster A is directly or indirectly connected to those clusters. The node having more number of structural holes plays a key role as it has vast information of the network and a fraudster tries to attack this node to access the information from this node.

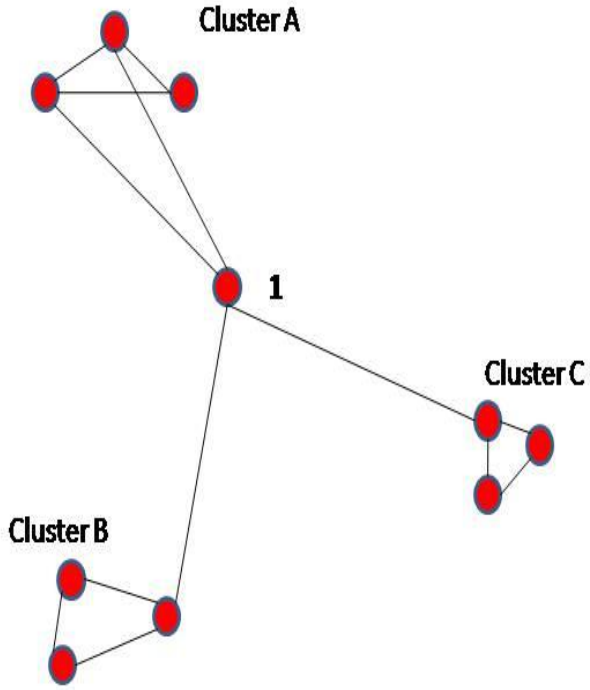

Figure 1.2 Structural hole

In figure 1.2, the social network has three different clusters A, B and C. In cluster A, node 1 is connected to two different clusters of the network so any kind of exchange of information will go through it. It has the information of all the nodes. If this node is removed from the network, three totally disconnected isolated clusters will remain in the network.

- **Some other measures**

There are certain other measures that are commonly used in social network analysis like sub-structures and clustering-coefficient. The major uses of these measures in social network analysis are network classification and network path prediction. Clustering coefficient gives the degree by which various nodes in the network lean to form a cluster. Sub-structures are used to analyze network data by grouping the nodes that are relatively closer to each other as compared to other nodes

- **Modularity**

Modularity is also an important metric of the structure of a social network graph. It is used to calculate the strength of a given network in groups. These groups may be later termed as clusters or communities. Higher the modularity of a network the more dense links will be present between the nodes in a single group or cluster but have lesser links between nodes present in different groups. It is mainly used for detecting community structure for optimizing the methods in a network. The limitation of modularity is unable to detect communities in a small network. Modularity is the ratio of the links within the cluster minus the expected ratio if the links are made at random. In figure 1.3 modularity classes has been visualized with the help Gephi software [41]. In it, different modules are clearly visualized. As it is observed from

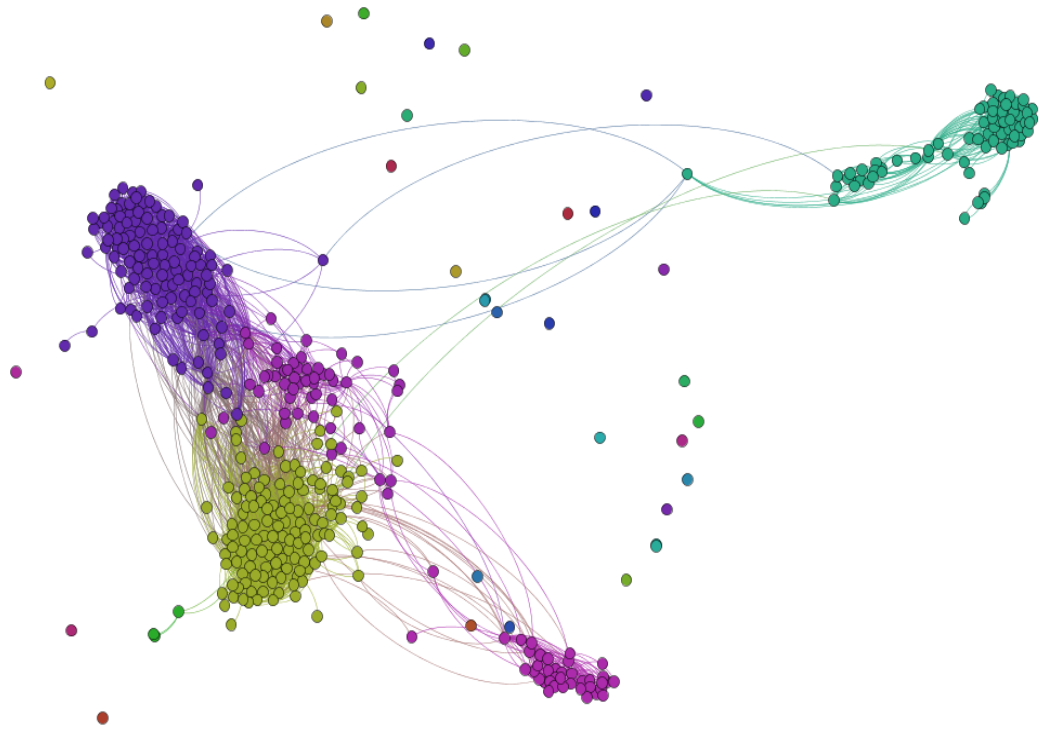

Figure 1.3 Groups formed on applying modularity

the figure that the green coloured module is away from other modules. It means the people present in that node hardly know the rest of the nodes in the network. In these types of graphs the presence of structural holes are more. Some of the nodes are isolated in it stating that these are the people having nothing in common with each other. The linking of these nodes is solely dependent on the person whose profile network it is.

1.3 Types of Social network

Whenever there is discussion about social networks the first things comes into mind is Facebook, twitter or Google+. But these websites does not cover the whole social network that exists. Social network is a very vast field and sometimes a part of social network overlap with the other part based on some characteristics. There are various forms of social network among which these are few of them.

- **Relationship network**

These networks are not the oldest one, but can define most of the networks. In these kinds of networks, a profile of the user is being maintained with extensive information about the user. This type of network allows us to keep all our information at one place commonly known as wall in Facebook. Relationship networks are different from professional networks where you can find work related information, share recommendations and you may connect to the professionals of the related field.

- **Media sharing network**

In this kind of network sharing the variety of media among the users is the primary goal. Instagram, Flickr are some examples of sharing media where images are being shared over a network. Media sharing network is extensively used by business organisations to do publicity about their products.

- **Online reviews**

A review is an appraisal of a product, company and movie or about some other things. Internet consists of vast knowledge and has a lot of consumers which usually choose to get an opinion to determine whether the product is good or bad. In present scenario, organizations have dedicated a team for addressing reviews of their products and try to entrust them with replying any query. Some fraudsters attack these networks and gave negative reviews on a higher rate which lead to decrease in the business rate of that particular organization.

- **Discussion forums**

It is the oldest types of social network. People can discuss about certain things in the form of posted messages that are publicly visible. Discussion forum networks commonly form a hierarchical or tree like structure. A single forum can contain different sub forums which may have different topics. Certain spammers utilize different techniques to post their spam having malicious content which may lead to risk the user.

- **Social publishing platforms**

This kind of network consists of blogs and micro-blogs, which are used to share different content. These platforms consist of real time interaction among users. Twitter is the most common example of this kind of platform. Most of the organizations keep blogs about their product to gain visibility and they use to create engaging content for their social channels.

- **Bookmarking sites**

In the present scenario, there is abundant of interesting, important and useful content online. Keeping track of each and every thing is like impossible. Bookmarking sites is the key answer to all these problems. These sites work like a store house where user used to store the content from the internet to their account. The user content can be made public and private. Based on the content stored, these sites will recommend the content similar to the stored one. There are various fraudsters who keep a track on this type of accounts to know the interests of the user and try to spend spam related to this type of content.

- **Internet based network**

In Internet based network, user can find different people having common interests, hobbies or location. Facebook, Google+ and LinkedIn are the major examples of this kind of network. For an organization, keeping account on this kind of network is a better place to share current trends among the followers of its products.

- **E-commerce**

E-commerce changed the trend of shopping things from different stores. It gives an ease to the customer to view and purchase products by just on a click. As everything is being shared on the network the chances of vulnerability also increases.

1.4 Anomaly detection in social network graphs

Graphs are more useful in capturing the long-range correlations among all the interdependent data objects [7]. There are various reasons of using graphs in anomaly detection in the network.

Inter-dependency of data: Data objects are mostly related to each other and show dependency. Almost all relational data is inter-dependent, which is responsible to account for linked objects in detecting anomalies. There are ample amount of datasets of this type such as social network, email and telephone networks, blogging networks.

Powerful portrayal of network: Graphs basically portrait the relation among nodes using edges between them. The various links lying in between these related nodes effectively stores their long-range correlation. A graph portrait ease the representation of rich datasets by introducing edges and nodes.

Relational nature: The nature of anomalies may display themselves as relational. Like in fraud domain, there may be two types of fraud i.e. opportunistic and organized. In opportunistic fraud, if one commits fraud there is higher probability of having the same kind of fraud from the related nodes. In an organized fraud, there is a tight collaboration of certain related group of particular subject.

Vigorous apparatus: Graphs are the most powerful and robust tools for analyzing the network. For a fraudster to fit in a particular network, a global view is required which help in understanding the structure and dynamic operations of the network.

1.5 Risks to the graph

A social network holds user's basic information and provides links between different people to share the information. The two main and basic properties of social graph are

- It stores all the information of the user over the network
- It provides a powerful platform to share information among different nodes.

Hence, the information stored on the network becomes the main target of the attackers. The attackers try to control or compromise the portion of graphs to gain the access in the graph. There are three root causes for it i.e. fake accounts, compromised accounts and creepers [8].

- **Fake accounts**

The concept of social networks is to share useful information with higher degree of ease. But as the growth of the network, many attackers try to hack the vital

information for personal/professional benefits. Some individuals create fake accounts just to have an extra account whereas some fake accounts are created intentionally for attacking persons by entering into their sub graph. These fake accounts can be created either by script or raw labour or as both. Basically, there are mainly three reasons for creating fake accounts by an attacker. These fake accounts are used to overcome the rate limits associated with per person account, to boost their ranking or trust and finally, used as fake identities to phish and spam real users. By catching fake accounts earlier in the life cycle is required.

- **Compromised accounts**

Compromised accounts are those accounts where the real owner of the account lost complete or partial control on the account. Attacker can gain access either by some phishing attack or by malware attack. Phishing attack can be traced by tracking and maintaining the logs of IP address. Malware is somehow hard to detect as the attacker is using the same machine.

A Phishing attack generally tries to gain the login credentials. They normally spread by compromising the user trust maintained in the graph. A successful phishing attack is harmful as it acquires a trusted node and then can gain access to all the credentials to exploit financial gains and can have any kind of information being propagated over a network. Commonly, the users over social network are more vulnerable as compared to e-mail users.

Malware is more complex than the phishing attack. It resides in the user's system. If the malware is installed on the user's system the attacker can easily steal the user session and use it on the behalf of the user. These malware normally works silently which helps them to avoid detection. The infected system thus can be used to propagate the virus infected messages over the network. The most general solution to avoid these kinds of attacks is to take user feedback over the sub network the malware is using to spread.

- **Creepers**

These are the real people on the networks who are used the network in an offended way which is problematic for the other user on the network. Most common kind of creeping action being performed by them is sending friend requests to strangers which results it as spam for the receiver. These creepers generally post spammy chain letters to have broad feed distribution. These chain letters can cause mainly two problems

either it motivate the user to take some damaging actions on this fake spammy post or can create a global misinformation which tend to suppress the critical or time sensitive information.

- **Spam**

It is the root of above three attacks in a social network. Being on social network, there are a lot of communication channels between different users. Generally, attackers keep a track of all the nodes to distribute spam and find out the weakest node having higher degree of connections. Declaring spam to a node on certain characteristics is a difficult task as the behaviour of the node may be acceptable on different region. Being on global user base, every sub structure has different social norms for communication. Hence to detect a spam both user feedback and automated system response is required.

1.6 Limitations of social network analysis

Performing social network analysis comes with some limitations. The deficiency of publicly availability of the data on which certain experiments can be performed and the lacks of generalized techniques to detect the fraudsters in the network, no hypothesis testing, and complexity limitations. There are some limitations related data and data processing. Data remodelling is necessary to keep the effectiveness of social network analysis as the observed volume of data increases. Database query may cause overheads due to the join operations performed on the huge dataset which may increase the detection time. Social network analysis is commonly reflective in nature which means action will be taken after the fraud happens due to fraudulent node. Social network analysis is not a modelling technique, the experience gained from observing a fraud network is beneficial and can be used to create an improved analytical models. There are certain social network analysis applications like UCINET, SAS Fraud Framework.

1.7 Structure of Thesis

The rest of the thesis is organized as follows:

- Chapter 2 illustrates the literature review.
- Chapter 3 defines the problem statement for the proposed work, its objective and research methodology.

- Chapter 4 introduces the proposed algorithm and certain factors used in the work which are the basics of our thesis.
- Chapter 5 gives the implementation and experimental results.
- Finally, chapter 6 gives the conclusion, summary and future scope of the work.

Chapter 2 Literature Review

In the present scenario, anomaly detection in social networks becomes competent area of research. The major goal of finding out anomalies is to identify the adaptive trends of suspicious activities in the network. From the past decades, designing a generalized method for anomaly detection is an exhaustive job. There are some well-developed methods for detecting anomaly under specific condition on different domains.

2.1 Anomaly detection

In a malware attack, the attackers make use of client's machine for spreading infected content. In [9], Von Ahn et al. gave a method to stop the autonomy of the malware infected system for sending messages. They introduce the new concept of CAPTCHA, which helps to distinguish human from autonomous machines. But this has the limitation that it can only handle the autonomous machines from spreading spam. It has no specific control over the malware being propagated by the humans i.e. attacker.

In [10], Shetty et al. directed the complications of important nodes and discovery of tightly coupled group among them. They also proposed basic way to calculate entropy of the graph as event based graph entropy. Betweenness centrality gives poor results when the network is a mixture of leaders and followers. The main aim is to find the influential nodes in the graph using event based entropy. The proposed algorithm is implemented on Enron dataset.

In [11], Chandola et al. grouped different already existing methods into different categories keeping the underlying approach in consideration. For every category, a unique identifier or characteristic is chosen which help in differentiating normal and suspicious behaviour. A basic anomaly detection technique of a particular domain is applied on the dataset and compares it with different existing techniques being applied on the same dataset. They categorize anomaly detection techniques into six categories: spectral analysis, statistical analysis, information theoretic, nearest neighbour, classification and clustering.

In [12], Bolton et al. uses statistical tools for the verification of author. Statistics and machine learning offers an efficient way for the detection of fraud or irregularities. It has been applied successfully in the areas of online transactions, money- laundering, telephonic network fraud and intrusion detection in computers.

In [13], Newman et al. gave two main aspects on the basis of which the social network can be differentiated from other networks which may be technological network or some biological network. They concluded that social network has non-trivial clustering and have assortative mixing or positive correlation among the degrees of adjacent vertices. Social networks are commonly grouped in communities and this grouping could account for observed clustering.

In [14], Shrivastava et al. gave two algorithms *GREEDY* which works on greedy set expansion and *TRWALK* is based on randomized graph traversal to detect attack sets. They formulated a class of attacks and termed it as Random Link attack (RLA) and explored it as a NP-complete problem. In Random Link Attack the attacker forms a set of fake identities and used them to interact with huge set of normal users. To detect RLA, the social network graph is being extracted and mined by applying these algorithms and the suspicious nodes are detected.

In [15], Akoglu et al. gave an effective method to detect offensive nodes or messages. They propose OddBall method which is unsupervised and faster to detect suspicious nodes in weighted graph and it does not require any user-defined constants. It maintains an outlier score for every node. To discover new patterns in the graph the major factors taken in consideration, such as patterns in density, weights, eigen-values and ranks.

In [16], Michael Fire et al. proposed an algorithm to detect anonymity in social networks. The false positive rate varies from 0.01 to .052 on various social networks. However, it is efficient only on small networks, for large networks addition of certain other features is required.

In [17], Chau et al. proposed a 2-Level Fraud Spotting which is used to detect fraudulent activities and the fraudsters. User level features are extracted like transaction being performed to get an idea of analysing the fraudsters. Network level features are used to capture the communication between various users. Both these features are combined to detect the irregularities using a Belief Propagation algorithm over a Markov Random Field.

In [18], Pandit et al. gave NetProbe model which is efficient as well as very effective for fraud detection. NetProbe's detection rate for fraudulent node is 90% and is less time consuming. It is used for static data, but if the data is dynamic Incremental NetProbe is used which is fast as compared to NetProbe. It works on the principle of belief propagation mechanism to find out the fraudulent nodes. The major advantage

of this model is that it detects the fraudulent nodes as well as predicts which node is likely going to commit fraud.

In [19], Akoglu et al. proposes a framework FraudEagle which explore the network to automatically detect fraudulent users and fake reviews in an online review network. The main aspect of this framework includes exploring the network effect among the users and products, unlike other which mainly consider the behavioural analysis. This framework includes two main steps i.e. scoring users and reviews for fraud detection. It is totally unsupervised which do not require any labelled data. It is scalable for very large scale datasets as its execution time increase with respect to the network size.

In this framework, if a customer is giving positive response to a product where other users are giving negative and vice –versa, that particular user is labelled as suspicious node or user.

In [20], Jindal et al. works on detecting opinion spam and trustworthiness of the opinions. In this, first of all duplicate reviews are detected and then type 2 and type 3 spam are targeted by using supervised learning having a labelled data. For detecting type 1 spam, it is difficult to create a labelled data for training. Hence, duplicate spam reviews are used for positive training and other as negative.

In [21], Welser et al. proposed a method to solve the coordination problems in a huge complicated task of assigning authorship. In this, the main focus is on Wikipedia pages where each individual has particular role within the network. A comparison is being performed between long term dedicated editors and a cohort of editor. The result shows that informal socialisation can provide role related labor instead growth and manipulation in Wikipedia.

In [22], Bird et al. mined five huge datasets and proposed an algorithm to find out their e-mail networks as the record of sub-groups. It has been noted that the existence of strong community structure within the pattern of their communication and it has much modular structure when the discussion aims directly on the source code artifacts.

In [23], Eberle et al. proposed three efficient algorithms for detection of anomalies considering all the major three graph changes i.e. label modifications, vertex/edge insertions and vertex/edge deletions. These algorithms use minimum description length principle to find the sub-structure which contains anomalous nodes and relationships. The major drawback of these three algorithms is the inefficiency of detecting anomalies if the dataset contains more than one type of anomaly. Suppose,

if an anomaly in the graph perform deletion and manipulation, it result in a pattern which is similar to the normative pattern. This results in missing the anomalous structure which is not analyzed by the GBAD-MDL algorithm. To overcome this, an alternative is used where GBAD-MDL algorithm is used with GBAD-P to detect this anomalous structure.

In [24], Hodge et al. gave variety of techniques used for outlier detection and compared them between other techniques. In this, a variety of techniques like full gamut of statistical, neural and machine learning techniques are discussed and have clearly shown that it is almost impossible to depend on a single technique to find the outliers in different datasets.

In [25], Priebe et al. uses theory of scan statistics on the network graphs by employing time series and inference methods for detecting anomalies in the graph. For getting more appropriate results one can use methods like variance stabilization, detrending and exponential smoothing. In this, the Enron dataset is used to as an experimental dataset and the potential use of scan statistics is demonstrated.

2.1.1 Static unlabelled anomalies

In this type of anomaly, when the behaviour of the nodes in the network shows some unusual behaviour, only the communication occurred between the nodes are considered and the labels of the entity and their relationship are ignored. In [26], Newman et al. discussed the various problems of finding community structure in networks. The community structure can be evaluated by benefit function commonly called as modularity. Therefore, communities can be detecting by analysing the network and finding the partitions in network having higher value of modularity. In this, modularity is being expressed in terms of eigen vector and eigen values of a matrix known as modularity matrix.

In [27], Miller et al. gave a framework where eigen vector L_1 norms of network's modularity matrix is used to find small, tightly bounded anomalous sub graphs. This framework works efficiently in finding sub graphs in signal processing context. The problem of detecting the suspicious sub graph is based on hypothesis test having

H0: the graph network is noisy (free from anomalous sub graph)

H1: the graph network is signal and noisy (anomalous sub graph is present)

In [28], Chakrabarti et al. proposed a model R-MAT (recursive matrix) used to formulate realistic graphs having basics of each and every node by analyzing very few parameters. R-MAT can formulate bipartite, weighted and directed graphs. In an

comparative analysis, the results generated by this model are similar to the power law behaviour and sometimes can be deviated from it. R-MAT has certain advantages over previous generators like the time complexity of building graphs is O(Elog(E)log(N)) time. It automatically forms graphs having "communities within communities" property. In this, AutoMat-fast algorithm is presented which is used to fit the parameters of this model.

In [29], Menges et al. proposed an agent based approach in an email social network where the individual maintains, establish and have the right of declining the links through e-mails. The model scheduler is based on the principle same as the working principle of Gillespie algorithm, which allows the actions self-scheduled based on the probability distribution. The graph generated by this model is the result of communication of different single agents; hence, the network is formed by bottom-up approach.

2.1.2 Static labelled anomalies

In this type of anomaly detection the labels of the entities and their relationship is considered. In [30], Gao et al. proposed an efficient solution to find out community outliers without considering links or community information. In this, a generative model called CODA is proposed that is able to detect communities and outliers based on hidden Markov's random fields. The data attributes related to each entity are designed using Gaussian distribution and relationships among entities are used to find out prior distributions over hidden labels.

In [31], Manish et al. proposed an efficient solution of evolutionary behaviour discovery. Network behaviour of a temporal dataset is monitored having certain communities and the odd ones are labelled as their behaviour is dramatically different from others. These entities are labelled as community trend outliers. In this, a two step method to find out community trend outliers is followed. Firstly, soft pattern mining is performed and then the detection of outliers is performed based on their deviation from normal behaviour. Based on various experiments it is observed that this model is highly effective and efficient in detecting meaningful community trend outliers.

In [32], Tsugawa et al. proposed an index called as LSI (Leadership Strength Index) which helps to find out the leaders in a community from social network. The properties of LSI are verified by applying it on log data of SourceForge. As in a community network leader plays an important role, the LSI may be used for inferring

leader's that are being in non-development communities. There exists a positive correlation between LSI and development statuses of open-source software.

In [33], Serin et al. proposed a technique to visualize and analyze the networks. The basic parameters used to detect the change in graph entropy are closeness, degree and betweenness. The basic principle used in it is Shannon's entropy model. The centrality measure is used to predict the sensitivity of the entity in the network.

In [34], Noble et al. introduced two methods for detection of anomalies in social network which are anomalous substructure detection and anomalous sub graph detection. The main objective of anomalous sub structure detection is to evaluate the whole graph and then find out the suspicious substructures embedded in it. In anomalous sub graph detection, subdue is used which helps in running multiple iterations on a single graph once set. As the iterations keeps on best structures are replaced by single vertex leading the less or suspicious sub structure behind.

2.1.3 Dynamic unlabelled anomalies

When the structure of the network changes with respect to time interval, the detection of anomalies is difficult to detect. In [35], Park et al. proposed a theory of scan statistics based on hyper-graphs. A hyper-graph handles the email data much better than a graph. The fact that hyper-graph handles e-mail data better because unlike graph, it stores all the recipients of a message in single hyper-edge, as in graphs for every recipient a separate edge is there. It helps in detections of anomalies by monitoring nodes and the number of messages sent by them.

In [36], Pincombe et al. introduces ten graph distance metrics which are used to create time series of the changes being held in the network by sequentially comparing graphs from adjacent time slots. These time series are modelled as autoregressive moving average (ARMA). Each time series is evaluated by ARMA model to detect anomalies by setting a residual thresholding.

In [37], Huang et al. proposed a link prediction approach to detect anomalies. In this, a framework is developed to detect anomalies in an email dataset using link prediction methods. A baseline random model is used, which is based on naive prediction given for link scores. Predicting links in a network helps in predicting the future communication based on earlier communications. The prediction algorithm is applied on the network and communication occurred for each pair is observed. The observed communication is compared with the predicted one and if there is a lot of variation for a particular node, that node is considered as anomalous node. The main focus is on

ego-nets, particular nodes keeping the node degree, size of the ego net in consideration.

In [38], Gyongi et al. discussed all the possible ways to select the seed from a web of pages over a network and then identifying the spam free pages from it. The result of getting good pages purely based on the seed selection. In this, a small set of seed pages is selected by experts. These selected seed pages are used to detect the other reputable pages over the network using the link structure. The pages which are associated with these selected seed pages are marked as good pages and thus propagated over the network. It is a kind of semi-automated technique as seed selection is a manual task. TrustRank can be used in search engines explicitly or it can be used along with page rank and some other metrics which are responsible for ranking the search results.

In [39], Fette et al. proposed a technique to detect phishing attach via emails with higher accuracy rate. To detect these phishing emails specialized filters are being used instead of basic spam filters. For building these specialized filters certain features will be added in the basic spam filter. These features are number of links of a particular node is monitored, number of domain to which the node is connected and number of dots. While detecting phishing mail and good mail, the rate of false positive and false negative will be kept separately.

In [40], Egele et al. presented a novel technique to detect compromised account on social network. A mixture of statistical model and anomaly detection is used to identify an account that shows a sudden change in the network. They developed a tool called as COMPA which implements this approach and can handle a large amount of datasets. The limitation of this tool is that if cannot detect the attacker if he post the messages that are of similar behaviour as of the compromised account.

Chapter 3 Research Problem

3.1 Problem Statement

With the abundant growth of social network, the amount of valuable data is also present over the network which can be accessed by the attackers if some security measures are not followed. In today's world, social networking sites becomes a basic need to access information and share ideas among others. Sharing your data over the network can be very dangerous if someone hack it from the network and use it illegally. To detect these fraudulent nodes in the social network is fundamental problem in the field of computer science. Many researchers proposed different techniques to overcome this problem. But as the social network is comprised of different domains, it is a tedious job to give a general solution to it.

Techniques have been developed to detect the compromised accounts and fake accounts in social networking sites. These techniques are not enough to identify the fraudulent nodes. There is need of monitoring each node continuously whenever it is active on the network and a log is maintained for every node which is somehow increases the complexity of the network.

3.2 Gap Analysis

Many algorithms are proposed to identify fraudulent nodes present in the social network but they are restricted to their domains. There are various tools presented by researchers which are autonomous and are used to detect fraudulent nodes like COMPA [40], but its limitation is unable to find out the fraudulent node if the attacker behaves like a normal user and propagates information which is actually a spam in the form of normal messages. Most of the techniques work when the network has attackers within it. There is a need to check the new nodes which enters in the network and all the nodes present in that network would get the knowledge about this node.

3.3 Objectives

As discussed above in research gaps following objectives has been considered.

1. To study, analyze and explore the existing anomaly detection techniques in social network.
2. To propose an algorithm for detection of fake/fraudulent nodes from the network.

3. To test and validate proposed methodology with the proposed algorithm of detection of fraudulent node from social network.

3.4 Research Methodology

The main aim of the thesis is to find out the fraudulent nodes from the social network. The methodology followed is:

- Strength of each node is calculated over the network from the relationship matrix
- A trust score is being calculated for each every node which is based on TrustRank [38].
- Based on the trust score and the strength of the node a class label is assigned to it.

Chapter 4 Proposed Work

Common social networking sites are under attack at every bunch of time from phishers, fraudsters and spammer. The main of these attackers is to enter into the network and then gain the information and expose the network to spread unwanted emails. In contrast, we formulize the problem of social network containing malicious nodes and anomaly detection algorithm. The metrics for assessing the efficacy of the proposed algorithm will be defined.

4.1 Preliminaries

4.1.1 Network Model

The social network is modelled as a graph G (V, E) having set V of N nodes and a set E containing the relationship or link between the nodes in the set V. In a real life scenario, a node is related to multiple different nodes.

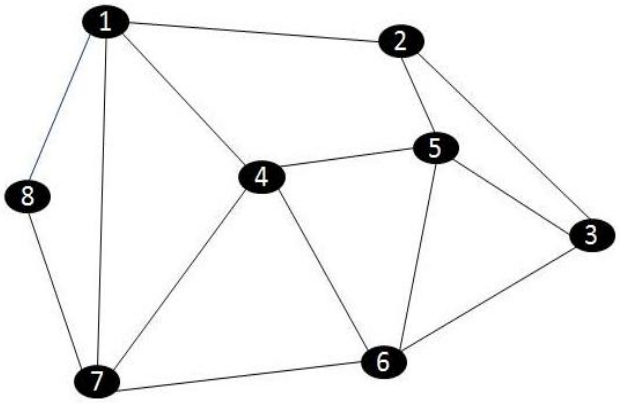

Figure 4.1 Social network graph

In social network, every node is linked with other node through a relationship. This relationship is formed either by sending request accepted by the receiver or by accepting the request from the user. In figure 4.1, a basic layout of social network is presented in the form of undirected graph. However, the number of accepted friend requests act as the in-degree of that particular node and the number of friend requests send by this node which are accepted acts as out-degree of the node. The nodes having zero in-degree and out-degree are isolated node in the network and cannot share anything over the network.

The matrix representation of a social network in fig 4.1 is:

Nodes	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0	1	0	1	0	0	1	1
2	1	0	1	0	1	0	0	0
3	0	1	0	0	1	1	0	0
4	1	0	0	0	1	1	1	0
5	0	1	1	1	0	1	0	0
6	0	0	1	1	1	0	1	0
7	1	0	0	1	0	1	0	1
8	1	0	0	0	0	0	1	0

Table 4.1 Matrix representation of an undirected social graph

4.1.2 Assigning ranks

Based on the behaviour of the nodes, a rank is assigned to every node in the network. The assignment of ranking is relying on the concept of PageRank. The main idea behind PageRank is a web link is considered as useful if various other useful links direct to it. The PageRank score r (p) of a web page p is given below:

$$r(p) = \propto \sum_{(q,p)\in E} \left(\frac{r(q)}{w(q)}\right) + (1-\propto)\frac{1}{N}$$

Where $\propto$ is a decay factor, w (q) is the out-degree of the page q.

The matrix equation of the above equation is:

$$r = \propto . M . r + (1-\propto).\frac{1}{N}$$

Where, M is the transition matrix. N is the nodes of the graph.

4.2 Estimating Trust

In the earlier stages, determining whether the node is fraudulent or not in social network is a subjective task. We offer the notion of checking the nodes by binary *Oracle function O* over all nodes n from the set of vertices.

$$O(n) = \begin{cases} 0 & if\ n\ \ is\ fraudulent \\ 1 & if\ \ \ n\ is\ a\ geniune \end{cases}$$

Oracle invocations are very time consuming and expensive over a large network. Thus, we skipped to use oracle function in our work. Thus, our main objective is to maintain an extra attribute with other attribute of nodes in social network. To detect genuine nodes we use approximation isolation of the genuine set of nodes. Genuine nodes are hardly connected to fraudulent nodes. However, some fraudsters got successful in entering the set of genuine node set.

4.2.1 Ideal Trust property

If the oracle function behaves ideally, then

$$M(n) = \Pr[O(n) = 1]$$

To demonstrate, let us take an example in which we have 100 nodes in a particular network are present and let us assume that all the nodes in this network has trust score equals to 0.6. After evaluating this network with oracle function and if M works quite properly, for around 60 nodes the oracle function would give value 1 and for the remaining 40 nodes the value would be 0.

In practical, achieving this kind of function is very difficult. However, it still gives some useful results and may give approximation to every node. Thus, if for a given link it calculates that node 1 has lower trust value than node 2, and then node 2 is likely to be more genuine. The properties of trust function is

- **Ordered Trust property**

The ordered trust property for a network is defined as:

$$M(n) < M(p) \leftrightarrow \Pr[O(n) = 1] < \Pr[O(p) = 1]$$

$$\mathrm{M(n)} = \mathrm{M(p)} \leftrightarrow \Pr[\mathrm{O(n)} = 1] = \Pr[\mathrm{O(p)} = 1]$$

- **Threshold trust property**

The threshold trust property is

$$\mathrm{M(n)} > \delta \leftrightarrow O(\mathrm{n}) = 1$$

If a node has score greater than δ, it is considered as legitimate node. This function helps us to tell at least the sub set of legitimate nodes from the superset.

4.3 Computing Trust Score

Calculating trust score over the network if the major aim of this thesis which in result helps in finding the fraudulent nodes. The trust calculation comprised of keeping the tracks of number of friend requests made over a network. A log is maintained for each and every node which stores the information of friend requests made, total numbers of requests accepted by the nodes send by this particular node.

For an example, let us consider a social network graph given in figure 4.2. The social network is represented as a directed graph showing which node has send request to other node and which node declined to accept the request by displaying it as a red colour link.

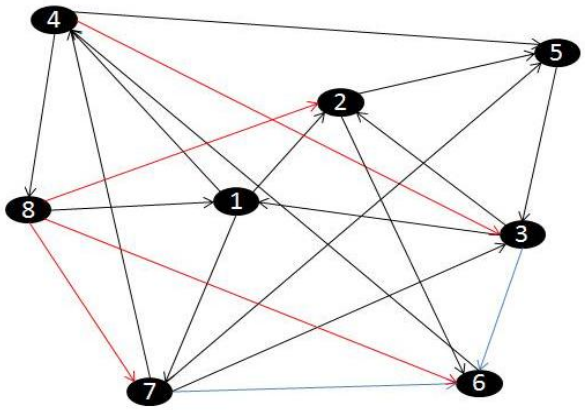

Figure 4.2 Graph representing friend requests accepted and rejected

Hence, to calculate the trust score of every node we use

$$Trust\ Score(T) = \frac{F_a}{Z_a}$$

Where, F_a is the number of friend request accepted by the nodes in the network which is being sent by the node 'a' and Z_a is the number of friend requests made by the node 'a'.

4.4 Computing the strength

The strength of the network in directed graph is calculated as summation of in-degree and out-degree. In our proposed work, directed graph has been taken into consideration, so we have to keep a record of in-degree and out-degree. The in-degree of the network is considered as the friend requests accepted by the node, whereas the out-degree is considered as the friend requests made by that particular node and are accepted by the corresponding nodes. If the strength of the node is greater than the half of the nodes present in the network, the node is considered as of higher strength. Strength of the network can be calculating simply from the adjacency matrix.

4.5 Fake_ID Algorithm

We have proposed an algorithm to detect fake identities over a network based on their trust score.

Algorithm: Fake_ID algorithm

Input:

M	Relationship Matrix
F_a	Number of friend requests accepted by the nodes
Z_a	Total number of friend requests sent over the network

Output:

Op	Fully genuine
	Moderate check required
	Fake account

Begin

/ if the node in the network has trust score NA then a manual check is required*/*

1. Calculate the strength of each node present in the network.

```
for i = 0 to N-1
        for j = 0 to N-1
                if( M[i][j]==1)
                        S[n_i] +=1
                end
        end
end
```

2. Calculate the trust score for each node.

$$\text{Trust Score(T)} = \frac{\text{Number of requests accepted } (F_a)}{\text{Total number of requests sent } (Z_a)}$$

3. Once the trust score is calculated it is being propagated over the network.

4. Each node is assigned a class number according to the strength and its trust score.

5.
```
if ( S> =N/2  &&  T >=  0.5 )
        Op=fully genuine
else if ( S< N/2 &&  T >=  0.5  )
        Op=moderate check required
else
        Op= fake account
```

End

In this algorithm, we assign label to each node and based on these labels one can detect which node is fraudulent and which is the genuine node. But sometimes some genuine node also possess some characteristics like the fraudulent node, therefore we make a class namely, moderate class in which a manual check is required before accepting the friend request from that person. This algorithm takes care of nodes at every level, whether the node is at entry level in the network or already present in the network.

In this algorithm, adjacency matrix of a social network is provided as an input where the information about the relationship between nodes is stored. The information about the number of friend requests sent and accepted among these is also required to detect the behaviour of the node.

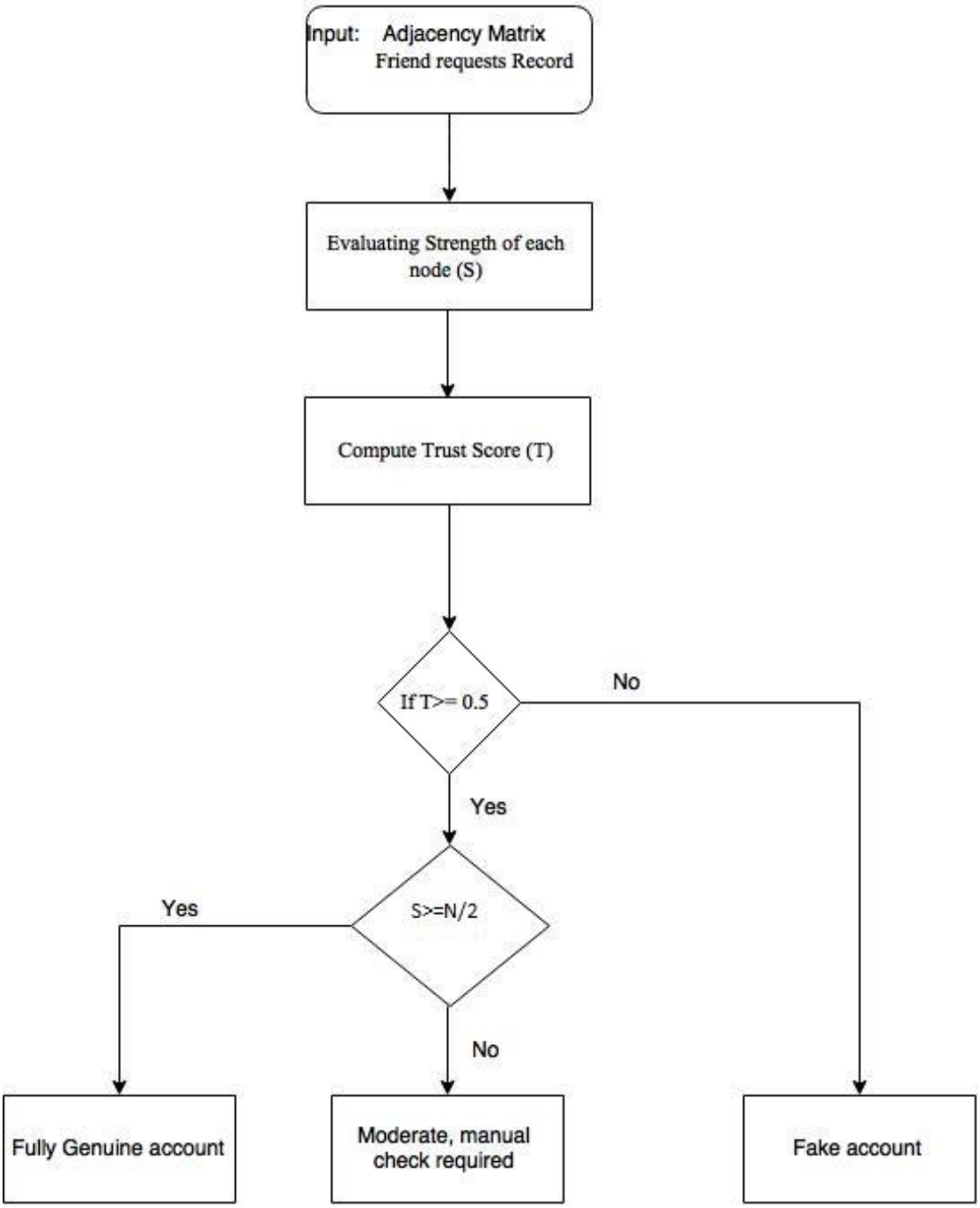

Figure 4.3: Flowchart of proposed algorithm.

Chapter 5 Implementation and Results

5.1 Implementation

In this section, the proposed algorithm in previous section is used to detect fake identities in the social network dataset. The new nodes joining the network will be assigned the trust score as 'NA'. On the basis of trust score and strength the class of the node or account is decided. The algorithm is developed in Java using NetBeans IDE 8.0.2.

The strength of the node depends upon the degree of the node. Higher the degree of the node leads to high strength of the node in the network. With the help of Gephi software [41], we demonstrated the degrees of the nodes in the network in figure 5.1. In this, we ignore the nodes having degree less than 10. The nodes with higher degree

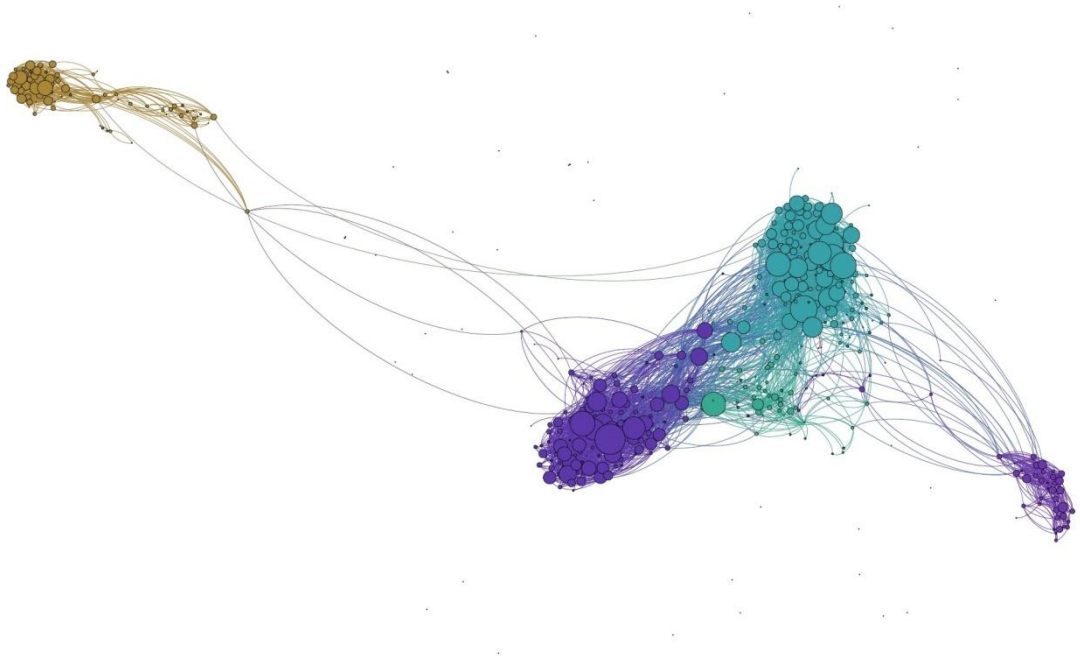

Figure 5.1: Representation of nodes based on their degrees.

than the average degree of the network are slighter bigger than the other nodes. These nodes play vital role in the network as they are responsible in forming clusters or modules. The fraudster will try to get linked with these nodes to gain maximum information from the network. In our work, we maintained a dynamic trust score calculation whenever there is any kind of request being made by the node and based on this activity we label that node the specific class name.

Let us take an example of a small dataset having 10 nodes and 26 edges or links between them. In figure 5.2, a directed graph is shown of the used dataset. The direction of the edge will define that which node has made the request and the colour of the node indicates that whether the request is accepted or not. The green colour of the nodes defines that the request is being accepted whereas the red colour defines the rejection of the request.

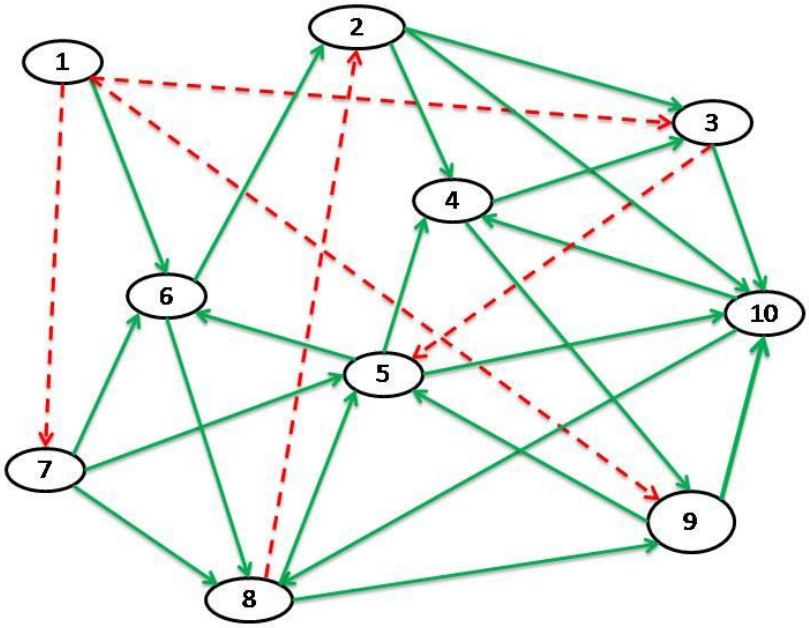

Figure 5.2: Directed Graph representation of the dataset

As in the figure above it is clearly visible that node 1 sent four friend requests and out of four requests three got rejected. Node 3 sends two friend requests and out of two, one got rejected.

As from the above information about the dataset, we can calculate the trust score of each node by calculating

$$\text{Trust Score(T)} = \frac{\text{Number of requests accepted } (F_a)}{\text{Total number of requests sent } (Z_a)}$$

The trust score of each node is given in table 5.1. The Trust Score equal or more than 0.5 is considered as a valid trust score for a particular node.

Node	Number of requests got accepted	Total number of requests send	Trust Score
Node 1	1	4	0.25
Node 2	3	3	1
Node 3	1	2	0.5
Node 4	2	2	1
Node 5	3	3	1
Node 6	2	2	1
Node 7	3	3	1
Node 8	2	3	0.66
Node 9	1	2	0.5
Node 10	2	2	1

Table 5.1: Trust Score of different nodes

On calculating the Trust Score of the node, the strength of the node is measured. If a node is new in the network the Trust Score will be 'NA' which distinguishes it from the fake nodes. The adjacency matrix of this social network is represented in Table 5.1.

Node	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	1	0	0	0	0
2	0	0	1	1	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	1
4	0	0	1	0	0	0	0	0	1	0
5	0	0	0	1	0	1	0	0	0	1
6	0	1	0	0	0	0	0	1	0	0
7	0	0	0	0	1	1	0	1	0	0
8	0	0	0	0	1	0	0	0	1	0
9	0	0	0	0	1	0	0	0	0	1
10	0	0	0	1	0	0	0	1	0	0

Table 5.2: Adjacency Matrix of directed social graph

After calculating the strength of every node in the network, it is compared with the Trust Score of that particular node and a class label is assigned to each node. The

class labels are assigned as fully genuine account, moderate account and fake account. The moderate account requires a manual checks as it satisfies some of the characteristics.

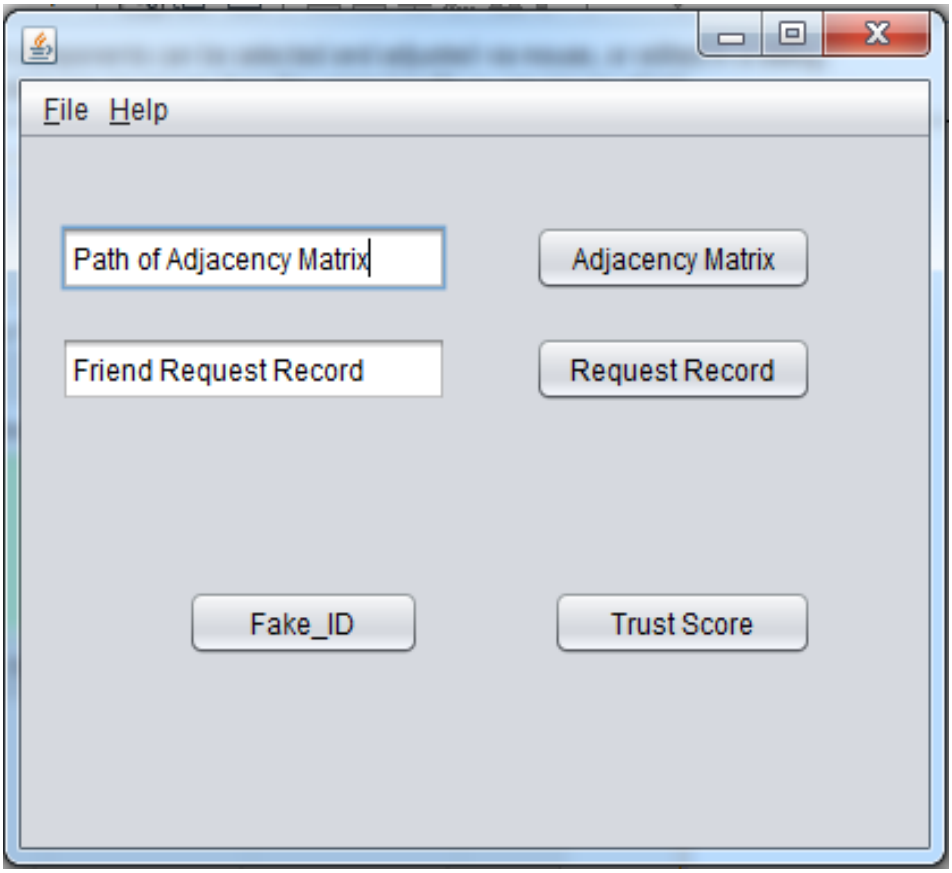

Figure 5.3: GUI of Fake_ID application

In figure 5.3, a layout of the application being developed is shown. In it, we have to input two matrices one regarding the information of the nodes in the form of adjacency matrix and the other one is the log containing information regarding the number of friend requests about each node.

After this, we can also calculate the Trust Score of the node by using button Trust Score button. It will display the Trust Score corresponding to the nodes present in the network.

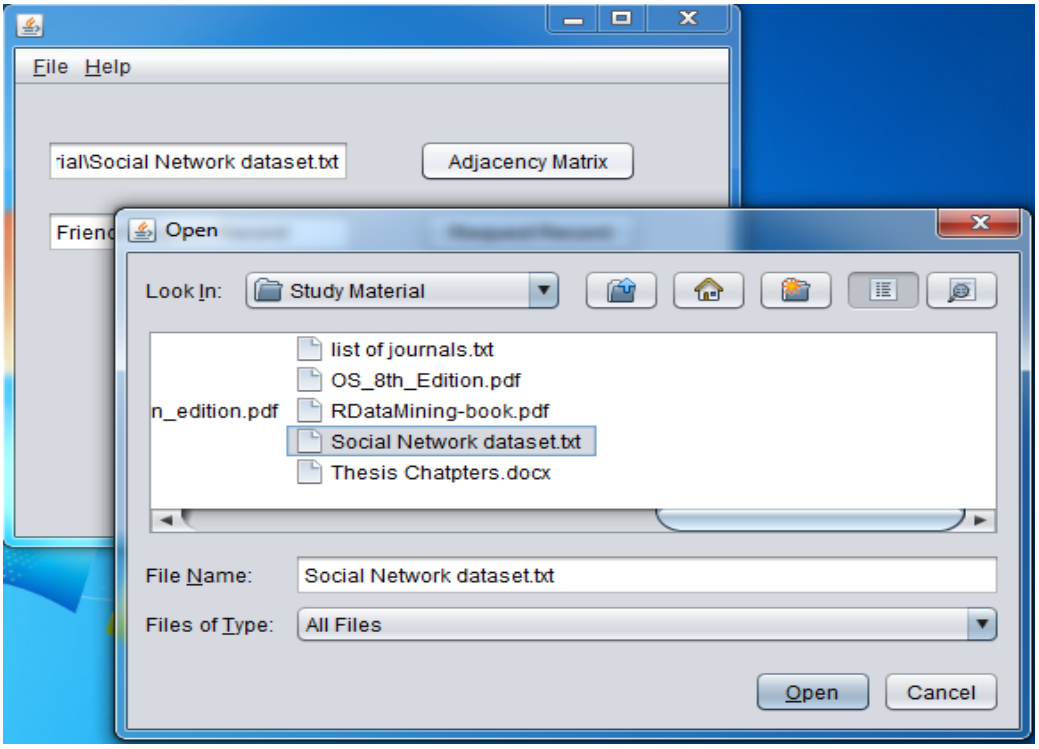

Figure 5.4: Adjacency Matrix file selected by user

If a link between two nodes is not present in the network zero is assigned. Whenever there is change in the network an updated file of the network dataset and request record is required. To validate the proposed algorithm, we take a manual dataset as in table 5.2 graphically represented in figure 5.2.

5.2 Results

On applying the proposed algorithm, it is easier to detect the fake node in the network. As the log record which is taken in consideration changes simultaneously based on the behaviour of the nodes, an active participation of this proposed algorithm is required. To reduce the complexity only two basic parameters are used. As the parameters are increased for detecting the fake accounts the complexity will also increase which is not desirable.

The trust Score of the dataset taken in example is shown in figure 5.5 and the class label of the nodes is shown in figure 5.6. The importance of assigning class label is that a normal user will be informed where he has to be aware before accepting the request from other user.

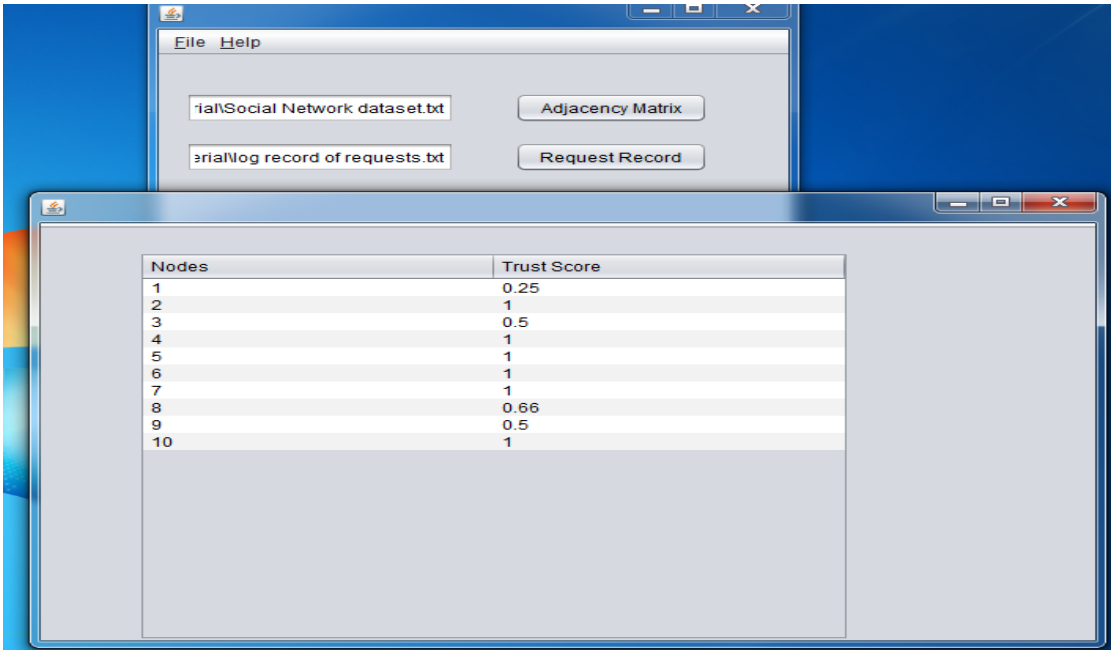

Figure 5.5 Trust Score of various nodes

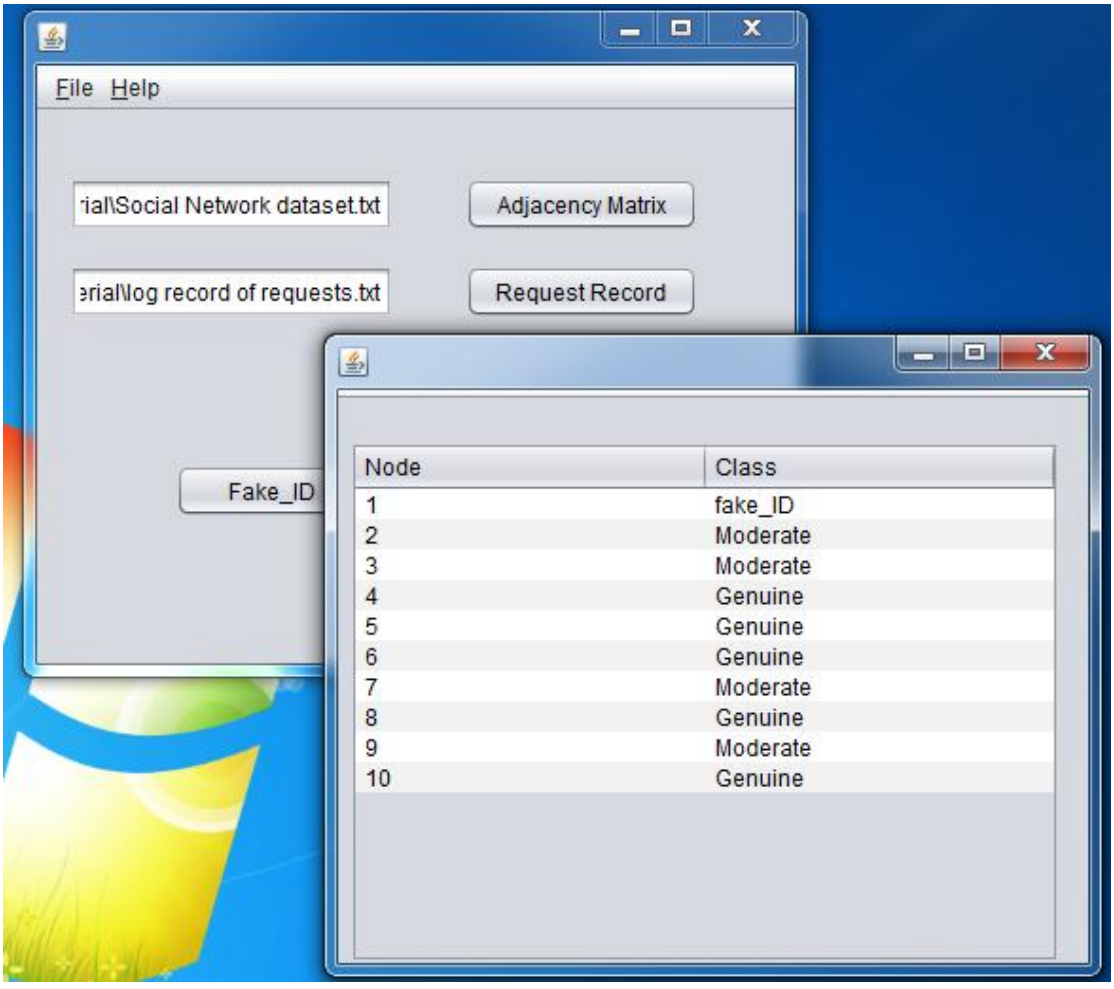

Figure 5.6: Detecting Fake nodes in the dataset

Finally, the proposed algorithm works efficiently in the domain of social networking sites network. We have various tools like COMPA which are working on detecting the compromised accounts and if an attacker has the knowledge of this tool, he can easily prevent himself from detecting. While in our technique, we are working on detection of the fake accounts which leads to elimination of fake nodes and have no longer access to the network as that particular node is labelled with fake ID.

Chapter 6 Conclusion and Future Scope

6.1 Conclusion

In this thesis an algorithm has been proposed to detect the malicious nodes or fake accounts from the social network. As the social network is growing exponentially, the chances of being hacked or information loss over the network is increasing simultaneously. Many algorithms are being proposed to detect the malicious or fake accounts over the network. Our main focus is on the way the node gets linked with other nodes. This algorithm keeps a check whenever there is a request made by any node of the network and the response to request is stored. A fake node always tries to connect to as much nodes as in the network to gain more and more information which can be used for illegal actions later on. Hence, by monitoring the behaviour of the node we can label nodes whether they are genuine, fake or moderate-in which a manual check is required.

6.2 Summary of Contribution

The major contribution attain by the work presented in the thesis are summarised as follows:

- A thorough survey of all the available techniques to detect fraudulent nodes in various domains of social network.
- On comparing these various techniques yield that they are domain specific and still a general approach to detect anomalies in social network is missing.
- Trust score and strength of the network is taken into consideration for detecting fraudulent node.
- On the basis of these two main attribute we try to make it as a generalized algorithm which assigns labels on the nodes whether it is genuine, fake or moderate.

6.3 Future Scope

In this work, fraudulent accounts are detected on analyzing only two basic parameters. Based on these, the given node is classified into a class out of three named classes. In this, a moderate class is also there when there is a possibility of false negative

condition. This class can be removed by taking some more useful parameters in consideration.

Apart from selecting these useful parameters, this algorithm can be extended to detect the online review system as there as various fraudulent accounts which tries to negate the reviews. Some major parameters like location and work place are also taken into consideration along with this to make more precise results.

References

[1]. Savage, David, Xiuzhen Zhang, Xinghuo Yu, Pauline Chou, and Qingmai Wang. "Anomaly detection in online social networks." *Social Networks* 39 (2014): 62-70.

[2]. Phua, Clifton, Vincent Lee, Kate Smith, and Ross Gayler. "A comprehensive survey of data mining-based fraud detection research." *arXiv preprint arXiv:1009.6119* (2010).

[3]. Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review."*Statistical science* (2002): 235-249.

[4]. Wolfe, Alvin W. "Social network analysis: Methods and applications." *American Ethnologist* 24.1 (1997): 219-220.

[5]. Chan, Kelvin, and Jay Liebowitz. "The synergy of social network analysis and knowledge mapping: a case study." *International journal of management and decision making* 7.1 (2005): 19-35.

[6]. Ehrlich, Kate, and Inga Carboni. "Inside social network analysis." *Boston College* (2005).

[7]. Akoglu, Leman, Hanghang Tong, and Danai Koutra. "Graph based anomaly detection and description: a survey." *Data Mining and Knowledge Discovery*29.3 (2014): 626-688.

[8]. Stein, Tao, Erdong Chen, and Karan Mangla. "Facebook immune system."*Proceedings of the 4th Workshop on Social Network Systems*. ACM, 2011.

[9]. Von Ahn, Luis, et al. "CAPTCHA: Using hard AI problems for security."*Advances in Cryptology—EUROCRYPT 2003*. Springer Berlin Heidelberg, 2003. 294-311.

[10]. Shetty, Jitesh, and Jafar Adibi. "Discovering important nodes through graph entropy the case of enron email database." *Proceedings of the 3rd international workshop on Link discovery*. ACM, 2005.

[11]. Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." *ACM computing surveys (CSUR)* 41.3 (2009): 15.

[12]. Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review."*Statistical science* (2002): 235-249.

[13]. Newman, Mark EJ, and Juyong Park. "Why social networks are different from other types of networks." *Physical Review E* 68.3 (2003): 036122.

[14]. Shrivastava, Nisheeth, Anirban Majumder, and Rajeev Rastogi. "Mining (social) network graphs to detect random link attacks." *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*. IEEE, 2008.

[15]. Akoglu, Leman, Mary McGlohon, and Christos Faloutsos. "Oddball: Spotting anomalies in weighted graphs." *Advances in Knowledge Discovery and Data Mining*. Springer Berlin Heidelberg, 2010. 410-421.

[16]. Fire, Michael, Gilad Katz, and Yuval Elovici. "Strangers intrusion detection-detecting spammers and fake proles in social networks based on topology anomalies." *HUMAN* 1.1 (2012): pp-26.

[17]. Chau, Duen Horng, Shashank Pandit, and Christos Faloutsos. "Detecting fraudulent personalities in networks of online auctioneers." *Knowledge Discovery in Databases: PKDD 2006*. Springer Berlin Heidelberg, 2006. 103-114.

[18]. Pandit, Shashank, Duen Horng Chau, Samuel Wang, and Christos Faloutsos NetProbe. "A Fast and Scalable System for Fraud Detection in Online Auction Networks Proceedings of the 16th international conference on World Wide Web (WWW'07). May 8-12, 2007." *Banff, Alberta, Canada*: 201-210.

[19]. Akoglu, Leman, Rishi Chandy, and Christos Faloutsos. "Opinion Fraud Detection in Online Reviews by Network Effects." *ICWSM* 13 (2013): 2-11.

[20]. Jindal, Nitin, and Bing Liu. "Opinion spam and analysis." *Proceedings of the 2008 International Conference on Web Search and Data Mining*. ACM, 2008.

[21]. Welser, Howard T., Dan Cosley, Gueorgi Kossinets, Austin Lin, Fedor Dokshin, Geri Gay, and Marc Smith. "Finding social roles in Wikipedia." In *Proceedings of the 2011 iConference*, pp. 122-129. ACM, 2011.

[22]. Bird, Christian, David Pattison, Raissa D'Souza, Vladimir Filkov, and Premkumar Devanbu. "Latent social structure in open source projects." In*Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering*, pp. 24-35. ACM, 2008.

[23]. Eberle, William, and Lawrence B. Holder. "Mining for Structural Anomalies in Graph-based Data." *DMIN*. 2007.

[24]. Hodge, Victoria J., and Jim Austin. "A survey of outlier detection methodologies." *Artificial Intelligence Review* 22.2 (2004): 85-126.

[25]. Priebe, Carey E., John M. Conroy, David J. Marchette, and Youngser Park. "Scan statistics on enron graphs." *Computational & Mathematical Organization Theory* 11, no. 3 (2005): 229-247.

[26]. Newman, Mark EJ. "Finding community structure in networks using the eigenvectors of matrices." *Physical review E* 74.3 (2006): 036104.

[27]. Miller, Benjamin, Nadya Bliss, and Patrick J. Wolfe. "Subgraph detection using eigenvector L1 norms." *Advances in Neural Information Processing Systems*. 2010.

[28]. Chakrabarti, Deepayan, Yiping Zhan, and Christos Faloutsos. "R-MAT: A Recursive Model for Graph Mining." *SDM*. Vol. 4. 2004.

[29]. Menges, Fabian, Bud Mishra, and Giuseppe Narzisi. "Modeling and simulation of e-mail social networks: a new stochastic agent-based approach."*Proceedings of the 40th Conference on Winter Simulation*. Winter Simulation Conference, 2008.

[30]. Gao, Jing, Feng Liang, Wei Fan, Chi Wang, Yizhou Sun, and Jiawei Han. "On community outliers and their efficient detection in information networks." In*Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 813-822. ACM, 2010.

[31]. Gupta, Manish, Jing Gao, Yizhou Sun, and Jiawei Han. "Community trend outlier detection using soft temporal pattern mining." In *Machine Learning and Knowledge Discovery in Databases*, pp. 692-708. Springer Berlin Heidelberg, 2012.

[32]. Tsugawa, Sho, Hiroyuki Ohsaki, and Makoto Imase. "Inferring success of online development communities: Application of graph entropy for quantifying leaders' involvement." In *Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on*, pp. 1-6. IEEE, 2010.

[33]. Serin, Ekrem, and Selim Balcisoy. "Entropy based sensitivity analysis and visualization of social networks." In *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*, pp. 1099-1104. IEEE, 2012.

[34]. Noble, Caleb C., and Diane J. Cook. "Graph-based anomaly detection." In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 631-636. ACM, 2003.

[35]. Park, Youngser, C. Priebe, D. Marchette, and Abdou Youssef. "Anomaly detection using scan statistics on time series hypergraphs." In *Link Analysis, Counterterrorism and Security (LACTS) Conference*, p. 9. 2009.

[36]. Pincombe, Brandon. "Anomaly detection in time series of graphs using arma processes." *ASOR BULLETIN* 24, no. 4 (2005).

[37]. Huang, Zan, and Daniel Dajun Zeng. "A Link Prediction Approach to Anomalous Email Detection." In *SMC*, pp. 1131-1136. 2006.

[38]. Gyöngyi, Zoltán, Hector Garcia-Molina, and Jan Pedersen. "Combating web spam with trustRank." In *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30*, pp. 576-587. VLDB Endowment, 2004.

[39]. Fette, Ian, Norman Sadeh, and Anthony Tomasic. "Learning to detect phishing emails." In *Proceedings of the 16th international conference on World Wide Web*, pp. 649-656. ACM, 2007.

[40]. Egele, Manuel, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. "COMPA: Detecting Compromised Accounts on Social Networks." In *NDSS*. 2013.

[41]. Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy. "Gephi: an open source software for exploring and manipulating networks." *ICWSM* 8 (2009): 361-362

List of Publications

1. Sushil Kumar, Ravinder Kumar, Karun Verma and Rajkumar Tekchandani "Fake_ID Algorithm for detecting fake nodes in social network." *National Academy Science Letters* (2015). [Communicated].

YouTube video link

The video link of the performed work can be accessed from

https://youtu.be/E7m5x1sIBdI

A personal reflection on my dissertation and research work is being described in this section. The journey of my research work started from second semester in ME-CSE at Thapar University, Patiala. I choose a topic from data mining field for my seminar. I haven't decided the topic of my thesis at that time. To give the seminar, I just read some of the ongoing topic in research and found data mining is one of the topic on which researcher are working from a long time. After studying data mining in our course work, my interest in this field keeps on going. Then, in third semester I choose topic from data mining in my project work.

January

After coming back from winter vacation, it's time to find a suitable topic for my dissertation. So, I decided to choose the topic from data mining as I was in touch with this area from past 5 months. I start reading about what major fields that are linked with data mining and was trying to sort out the field to precede. I start reading basics of every concern field and read about six research papers. Then I discussed it with my guide and go for Social Network Analysis (SNA).

Now, my topic is decided i.e. SNA. I started reading about all the basic about this and try to find out the gaps present in this area. Then, I read a research paper which is about "Anomaly detection in online social networks" written by Savage, David, et al. (2014). From here, my research area becomes fraud detection in social networks.

February

After deciding the area of my dissertation, I read almost everything about the frauds being performed in the network and the techniques proposed by various researchers for the detection of the fraud. The major drawback of all these techniques which I observed is that none of them works on the principle of generality. Each technique is specific for particular domain.

I decided to work on generality and try to build a technique which works for every domain. I try to find out the solution about this. But after trying so many possible ways for detection of fraudulent node, I observed that they are not working on my expectations.

March

After failure in finding out generality in these different domains, I start reading about the basic parameters of these domains. After studying these domains, I observed that each has different parameters and to generalize it we have to consider all these parameters which make it too much complex. If we consider all these parameters, the time complexity to detect the fraudulent nodes becomes too much high which is undesirable. I started studying more about social networks and the ways the attackers attack on a network.

April

In the first week, I read about some major techniques to detect the fraudsters. I found them that all are working on same principle that if the attacker shows a lot of variation in the behaviour as compared to the other nodes. But if the fraudster act as a normal node and distribute spam in the form of messages, these techniques are unable to detect them.

Some of the techniques I found interesting in this field are OddBall, FraudEagle and COMPA tool and Trust Rank algorithm for web pages. All these monitor the behaviour of the node in the network.

May

After studying about all these tools, I thought to find convenient method to detect these fake nodes. I start thinking how they originate? How they enter into the network?

After analyzing, I observed that the common user is unaware from the network and sometimes accepts requests without knowing that particular person. They do not have much knowledge about the fraudsters. If they find something interesting in their profile, they accept the request and the problem starts here. The fraudsters have acquired the access to the network. So, I decided to gave a solution such that the common user over the network will get to know about the fraudster even before accepting the friend request.

June

In this month, as the problem statement is clear to me, I worked hard to figure out the solution. Then, I came up with a solution while studying an article about data mining in which classification of certain items is being done. Then I used it in my solution where is used to calculate the strength and trust score of each node. Based on these two principles I assign different classes i.e. genuine, moderate and fake accounts to the nodes present in the network. So, it is easier for the user to find out which mode is the fraudster. Now, I started my coding section for this solution, which too has certain ups and down as how to read the network data, calculate the trust score for every node.

July

As it is the submission time, I completed all the pending work of my thesis which includes PowerPoint presentation, video and poster.