# Social Network Security Using Edge Removal Method

**Arun Dabas**

Lecturer
Delhi Skill and Entrepreneurship University (DSEU) , Dwarka Campus, New Delhi, India
(Formerly Integrated Institute of Technology, Dwarka, New Delhi)

***Abstract*: The security of social networks has become a challenge to the bonafide and honest world of online social network users. The recent instability in different parts of the world is one example of it. Every day there are news of different kind of wrongdoings in which social media is used as a tool to make strategies of wrongdoings and many times the government had to think of closing down internet services to stop unwanted or fake communication over social media using internet services. To tackle such situations it is very difficult to control the things manually. Sometimes the intensity of threat is so huge that even the concerned authorities are forced to think and take necessary measures in it. The social media sites are also no exception. To tackle such situations it is very difficult for the social media sites to take stringent steps merely on the basis of suspicions and to remove such users out of the network. Such acts have different theories not to do so. The manual control over the social media access is beyond consideration. The proposed work is to develop a system which can tackle this situation and may help the social network mechanism as well as the stake holders to tackle this situation in a secure and controlled manner.**

**Categories and Subject Descriptors :**Design

**General Terms:** Algorithm, theory, method, Social Network, Social Media

**Keywords:** Social Network, Edge Removal , Security, Design

## 1. INTRODUCTION

In the recent years the security of Social Networks has become one of the most difficult tasks to handle for the Social Network site managers. Attempts are being made to control the attacks on social network sites. Most of the attempts to identify antisocial identities are based on the relationship with other members in the social network.

Generally malicious users create fake identities in one form or another. Using these fake identities they post different kind of messages to execute catastrophic tasks. These tasks involved such as trolling, bullying discredit of respected persons of the society and spread rumors etc.. Most of the people execute such activities using fake identities these are just imaginary identities. Multiple identities are created for the same entity with false with false parameters. Impersonation identity is identity theft, it could be either stolen identity or identity created by someone else other than the genuine user. The reason is to create fake identity to perform malicious activities and to avoid real identification coming into picture. Another reason to create malicious identity is that many users want to keep their identity secret because they are afraid of misuse of their identity. Hence they create fake identity. Different practices are used by different authors to identify and manage malicious identities. One method to identify the malicious identities is to start from trust node and keep monitoring the credibility of each node of the network by visiting every node with respect to previous node. If any node found to be suspicious during crawling, it is marked as the malicious node and this process continues until all the nodes in the network are not visited. Another method adopted to identify the malicious identities is rank based. In rank based method the social network is traversed and each node is provided with a rank based on some parameters. Based on the rank values malicious nodes are identified, based on this, nodes are either accepted in the network or rejected from the network. The problem with the first method is that, based on the relationship between nodes, it is difficult to identify the real Malicious nodes. The relations have their own limitations to act. And hence it provides inaccurate results. So in this method the malicious identities are not precisely identified. For instance if two close friends exists in the network and they are linked with each other and suppose they do not interact frequently for one reason or other. In this manner the relationship between two close friends may not be analyzed properly and based on this relationship criteria, one friend may be wrongly analyzed as malicious. In the other method, which adopts rank based criteria to identify the malicious nodes has the rank problem. It is difficult to measure the exact rank to differentiate between malicious and honest nodes. Determining the accurate rank limits is basis of this method. If the rank criteria are not appropriate in that case the accuracy in identification of malicious nodes is quite discouraging.

We suggest in this paper a method, which suggests identifying and managing fake nodes in a social network and remove or discard their edges from the connected nodes so that the interaction among such identities is eliminated. And a secure network may be ensured.

The next section defines motivation behind my work, and section 3 defines my model in detail, section 4 specifies proposed algorithm and section 5 provides conclusion and future work.

## 2. MOTIVATION BEHIND THIS WORK

The area of social networking is growing extremely fast. Almost every domain related to human interaction and information sharing is taking help of social media. With the increasing popularity many people are indulging into bad practices and misuse social network sites or social media as a whole.

The honest users are always on the threat and the malicious users take advantage of lenient policies and network sites keep on indulging into such activities. Social networking sites, such as MySpace, Facebook, Flickr ,LinkedIn and instagram are becoming increasingly popular by the day. With some estimated 4.2 billion or more people are using social media in the current year, these users belonging to such sites, the opportunities for malicious users to act are unlimited and they execute these activities.The impersonation identity on social network sites has become quite common and it has become quite difficult to tackle such user. Bonafide users are bound to restrict their usage.

The people have adopted new means and methods to interact among themselves. With the popularity of smart hand held gadgets such as smart phones and ipads the popularity of social network sites has increased drastically. Since most of the mobile phones and other hand held devices contain internet connection and inbuilt social network applications so more and more people prefer to use social networks for interaction as a convenient tool to be in touch.

## 3. METHODOLOGY

The social networks are formed by nodes as members connected with edges as their relations. These nodes are connected with each other in such a way that they form communities based on certain common factors.

Our approach uses Breadth First Search Traversal method for traversing purpose and then dual weight method to segregate nodes.

The Breadth First Search Traversal Algorithm

Given a graph G = (V, E) with vertex set V =V(G) and edge set E = E(G),

The BFS is used to compute for each vertex $v \in V$ the weight v.wt that v lies from a distinguished source vertex $v_0 \in V$. the weight is measured as minimum number of edges on a path from $v_0$ to v in G. For this the FIFO queue is used as a data structure.

The algorithm operates on a graph G with source vertex $v_0 \in V$ (G). The algorithm is implemented using a FIFO queue Q as main data structure to compute for each $v \in V(G)$ its weight v.wt from $v_0$.

In our approach we traverse nodes using BFS algorithm to identify malicious identities preferably community wise. Every time if we find any node resemble with malicious criterion based on dual weight method, we de-link the edge of suspicious node from the honest node or prune that node from the honest node depending upon the criteria as shown in fig.

Fig 1 Deletion of Malicious edge

It may be possible that the node considered being Malicious might have more than one edge connection. In that case it would be de-linked with maximum threat or minimum credibility with the node.

Besides other parameters, at the time of creation, each node contains

- A pre-assigned weight c_wt = say 5
  This weight will also measure the credibility of that node from time to time. This pre-assigned weight (credibility) changes with respect to interaction of node with other nodes and the response thereof.
- Second pre-assigned weight t_wt = say 0, 1, 2,3,4,5 depending upon the relation and trust level. This weight is also treated as trust weight among nodes in the social network. Based on this weight, the friendship or closeness among nodes is measured.
- On every occasion a node sends request to another node for friendship, depending upon friendship node's response, the credibility of requesting node increases or decreases. Every time a request is rejected, the credibility factor is decreased by 1. This credibility factor could lead up to (-5). And every time a request is accepted the credibility factor is increased by 1. This could go up to (+5).
- To detect malicious node, we start with any trusted node. Keep on traversing the graph and find the malicious node. Once a node is suspicious to be malicious, we take appropriate action on that node such as whether to remove the edge or to prune the node.
- We compare the node with all connected edges, if calculated sum c_wt + t_wt < 2, it means the credibility of the node is below secure parameters and hence the connected edge is removed. If the calculated sum c_wt+t_wt < = 0 , in that case it may be ascertained that the node is definitely Malicious node and needs to be pruned.

- This process of analyzing and evaluating nodes and edges is a continuous process and ensures that all the nodes in the network have been visited analyzed. This process evaluates the changing behavior of nodes and edges in term of their weight based on different actions and accordingly appropriate rule is applied on nodes and edges.

- I have used GUESS graph exploration analysis tool to analyse the functioning of my algorithm.

## 4. PROPOSED ALGORITHM

1. Start
2. Assign Friendship strength at time of creation of node range 1-5

   # Besides other parameters, each node contains at the time of creation

2. c_wt =5 /* pre-assigned weight
3 .t_wt = 0 /* pre-assigned trust weight
4. Start analyzing with any trusted node in the network
5. do while (every node is visited) /* traverse every node
6. max_wt =0
7. If t_wt < 2 {

   Compare t_wt of this node with all connected edges

   max_wt = min(t_wt)

8. if max_wt < 2 {

   /* store node info with connected node as c_node

   If (t_wt <=1 )

   Prune(g.edge)

   else

   Visit next connected node

   t_wt = t_wt + 1

   }
9. If request made by node is rejected by requested node

   Then decrement weight by one (i.e. t_wt =t_wt-1)

   Else

   visit next node
10. Place g.node
11. Link g.node with c.node

## 5. CONCLUSION AND FUTURE WORK

We have tried to identify the malicious users on the social network sites based on their interaction with other users and behavior on the social network site. Due to certain reasons it is quite difficult to delete or eliminate the account of malicious users instead we remove their edge from connected with different users. Such users remain in the network without any connection with so-called honest users. And hence this spiral problem is addressed. However the performance of the model cannot be measured as 100 percent, but upto certain extent fake users may be identifies and their pattern may be observed.

In future I propose to make this model more flexible with enhanced performance and to use live data to test the accuracy of the model and based on the live data results any modification may be executed if required. The proposed live data is planned to be obtained from local communities network of a university, college or any organization depending upon their operational policies of that organization.

**REFERENCES**


[1] Maping search in Social Networks : Jonathan Haynes , Dept. of Sociology , Univ. of Stanford
[2] Expanding Network Communities ANDREW MEHLER and STEVEN SKIENA Stony Brook University
[3] Community Detection in Large-Scale Social Networks :Nan Du , Bin Wu, Beijing University
[4] Anonymous Opinion Exchange over Untrusted Social Networks Mouna Kacimi Max Planck Institute for Informatics Saarbrucken, Germany
[5] Characterizing User Behavior in Online Social Networks Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern/Saarbrücken, Germany
[6] An anlysis of social network base malicious defensesBimal Vishwanathan, K.P. Gummadi
[7] A Near – Optimal Social Network Defense against Malicious attacks Haifeng Yu , Michael Kaminsky
[8] Christopher C. Yang , College of Information Science and Technology, Drexel University , 1-4244-2415-3/08 IEEE
[9] Bageshree Shevade , Hari Sundaram (arts Media and Engineering, Arizona State University) , Lexing Xie IBM TJ Watson Research Centre
e-mail (bageshree.shevade, hari.sundaram) @ asu.edu , xlx@us.ibm.com
[10] Terrorism and crime related weblog social network : Link, content analysis and information visualization.
Christopher C. Yang and Tobun D. Ng (yang@se.cuhk.edu.hk) 1-4244-1330-3/07 IEEE
[11] B.A Nardi , D.J. Schiano, M. Gumbrecht and L. Swartz, "Why we Blog", Communication of the ACM, 47(12), December, 2004, pp.41-46
[12] Using an Edge-dual Graph and k-connectivity to Identify Strong Connections in Social Networks.
Li Ding and Brandon Dixon University of Albama, Tuscaloosa, AL 35487-0290, iding@cs.us.edu, dixon@cs.ua.edu ACM-SE '08
[13] Theft Gang Discovery using co-offending knowledge and SNA
Fatih OZGUL, Chris BOWERMAN, School of Computing and Technology, University of Sunderland,
[14] Dynamic Social Network Analysis of a Dark Network : Identifying Significant Facilitator, Sidharth Kaza, Danning Hu, and Hsinchun Chen, Fellow IEEE.
1-4244-1330-3/07 IEEE
[15] MaliciousInfer: Detecting Malicious Nodes using Social Networks George Danezis Microsoft Research,Cambridge, UK. gdane@microsoft.com
Prateek Mittal,University of Illinois at Urbana-Champaign, Illinois, USA. ,mittal2@uiuc.edu
[16] MaliciousGuard: Defending Against Malicious Attacks via Social Networks Haifeng Yu Michael Kaminsky Phillip B. Gibbons Abraham Flaxman
[17] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
[18] http://graphexploration.cond.org/