International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

A Study on Large-scale Social Tagging Behavior of User in Online Social Network

[1]S.Monika, [2]C.Anand

[1]PG scholar,[2]Assistant Professor, Department of Information Technology, K.S.R.College of Engineering

Received: 17-06-2015, **Revised:** 02-08-2015, **Accepted:** 13-10-2015, **Published online:** 01-12-2015

ABSTRACT

Online social networks equally referred as Facebook, Twitter, Google+, LinkedIn and Foursquare have become majorly democratic all over the world. A social network represents a significant role in people's daily life by building social relations among people. Nowadays people can access these social networks using both desktop PCs and new emerging mobile devices. With billions of users worldwide, Online Social Networks are a new venue of innovation with many challenging research problems. An understanding of user interactions in OSNs can provide important insights into questions of human social behavior and the pattern of social platforms and applications. In this paper, a study on user behavior in OSNs from several perspectives like connectivity and interaction among users, traffic activity, social tagging, mobile social behavior is considered. Also, this paper study malicious behaviors of OSN users and discuss several solutions to detect misbehaving users. This paper explores existing research highlights and provides various needs of significant research in these topics.

Keywords - **Anonymity, Clickstream, Crawling, Privacy, Online Social Networks, Sybil defense**

1. INTRODUCTION

Online social networks (OSNs) have become majorly democratic. According to Nielsen Online research [1], social media is the most popular online activity. It has pulled out email. More than two-thirds of the global online population access social networks and blogs. In fact, social networking account for nearly 10% of all time spent on the Internet. This shows that Online Social Networks play a vital role in global online experience. So this makes the study on user behavior in OSN important. It is important for Internet Service Providers to have better understanding of these network activities in order to resolve challenging problems seen today in OSNs, between end users and OSN sites [2]. The rapid growth of OSNs has attracted a large number of researchers to explore and study this popular and large-scale service. In this paper, a study on user behavior is done from several perspectives.

The first section discusses the aspect of connectivity and interaction, based on four different types of social graphs. A social graph is a classic and effective mathematical model to present the relationship between users in OSNs, and has been widely used in OSN research. In this paper, we search a deeper understanding of both visible and latent user interactions in OSNs. The second section discuss about mobile social behavior. Nowadays, web applications have been expanded to mobile platforms, for the compactness of users. Many Online Social Networks can be accessed using mobile phones. In this section, we focus on studies of user behaviors and improving the system efficiency of MSN systems.

In the third section, study of user behavior on the perspective of traffic activity is discussed. In the past, social network analysis was the domain of sociologists and anthropologists. Their typical tools are surveys and interviews which have the drawback that they can usually only capture a small user base. Nowadays, with the advent of online social networks, the networking community is capable of gathering large scale data sets from OSNs. Traffic activity is analyzed using these data sets. This section provides us with a method to understand the network usage of OSNs. The fourth section discuss on user behavior of OSN from a social tagging perspective. This section studies how privacy is affected by social tagging.

The fifth section discuss on malicious attacks in OSNs. This paper mainly focuses on malicious behavior in OSNs, including spam and Sybil attacks. Online social networks (OSNs) are popular collaboration and communication tools for millions of users and their friends. Unfortunately, in the wrong hands, they are also effective tools for executing spam campaigns and spreading malware. This section discusses several solutions to detect misbehaving users. Understanding OSN user behavior is important to different Internet entities in several aspects. This paper guide Internet Service Providers to do some infrastructural actions like addition of traffic optimization in network middle-boxes. This study helps

- OSN service providers to understand their customers' attitudes toward different experimental functions.
- OSN service providers to understand locations which are most cost-effective to build data centers or which content delivery network (CDN) cluster could be leveraged to deliver frequently accessed data.
- Users to enhance user experience.
- To detect misbehaving users.

2. CONNECTIVITY AND INTERACTION

The social graph is an effective and widely-used mathematical tool to represent the relationships among users in OSNs. Social graphs are used to analyze social interactions and user behavior characterizations. The use of social graphs imparts meaning to online social links by quantifying user interactions. Social networks can be modeled as undirected graph or directed graphs. Friendship graph and interaction graph are undirected graph. Latent graph and following graph are directed graph. Table 1 lists four different types of social graphs. Based on these graph types, this paper discusses the connectivity and interaction among OSN users. In this section, analysis, and modeling works related to the social graph is done.

Table 1: Four different types of Graph

TYPE	EDGE
Friendship graph	Friendship between users
Interaction graph	Visible interaction, such as posting on Wall
Latent graph	Latent interaction, such as browsing Profile
Following graph	Subscribe to receive all messages

2.1 EXISTING SOLUTIONS

2.1.1 DIRECTED GRAPH MODEL

Latent graph and following graph are directed graph.

Latent graph—A majority of user interactions on OSNs are *latent interactions*. Lateral interactions are passive actions such as profile browsing that cannot be observed by traditional measurement techniques. Online social networks (OSNs) not only provide interaction and communication, but can alter the way users interact with the network. From recent survey, Facebook has more than one billion active users and is the most visited site on the Internet. Increasingly, Facebook and Twitter are replacing email and search engines as users' default interfaces to the Internet. Online Social Networks like Facebook and Twitter is giving sites access to information about their visitors and their friends, through new platforms such as Open Graph. Jiang *et al.* [3] study latent interactions based on the crawled data of Renren, the largest OSN in China. It is the oldest OSN too. Renren can be best characterized as Facebook's Chinese twin, with most of Facebook's features and a similar user interface.

For their article, they used crawled data of the entire Renren network from April 2009 to June 2009, and again from September to November of 2009. They seed crawlers with some most popular users' profiles, and performed a breadth first traversal of the social graph. They collected unique user IDs, network affiliations, and friendship links to other users. They used data from the last crawl, which was an exhaustive snapshot that included 42,115,509 users and 1,657,273,875 friendship links. Renren tracks the most recent nine visitors to every user's profile, and makes the measurement of latent interactions possible. In a *latent graph*, a directed edge from one node representing a user to other node representing another user indicates the first user has visited second user's profile. Therefore, the in-degree of a node shows the number of visitors to that profile; while the out-degree reveals the number of profiles that user has visited. Based on Renren's crawled data, a comparison between latent interactions and visible interactions is conducted. There were 42 million users and 1.66 billion social links. There are three major findings.

- Latent interactions are significantly more prevalent and frequent than visible interactions.
- Latent interactions are non-reciprocal in nature.
- The profile popularity is uncorrelated with the frequency of content updates or number of friends for very popular users.

Following graph—Twitter is the world's largest micro blogging service .The majority of trending topics in Twitter are headline or persistent news in nature. Hwak *et al.* [4] perform extensive measurement on Twitter and reveals its power in information spreading on the news media level. Twitter users tweet about any topic and follow others to receive their tweets. The goal of article was to study the topological characteristics of Twitter and its power as a new medium of sharing the information. Crawled data of the entire Twitter site was obtained and also obtained 41:7 million user profiles, 1:47 billion social relations, 4,262 trending topics and 106 million tweets. It introduces a directed graph model to give an overview of Twitter's distribution of followers/ followees, and analyzes how the number of followers or followees affects the number of tweets. In Twitter's *following graph*, a directed edge from one node representing a user to another node representing another user indicates first user has subscribed to receive second user's latest messages. This article tries to list the users based on followers, page rank and retweets. The top users in the rankings are either celebrities or news media accounts. This article also compares Twitter with other media. The graph reveals Twitter's live broadcasting nature.

2.1.2 UNDIRECTED GRAPH MODEL

Friendship graph and interaction graph are directed graph.

Friendship graph— Social networks provide communication, storage and social applications for billions of users. Users can join and establish social links to friends. They make use of their social links to share content, organize events, share comments and search for specific users or shared resources. In friendship graph, every user is denoted as a node, and the friendship between any user pair is represented by an edge.

Interaction graph— Wilson *et al.* [5] try to find out whether social links are valid indicators of user interactions. Wall posts and comments shows whether the friends in social network interact each other. Based on the crawled data from Facebook, they have found that users interact mostly with only a small number of their friends, while often having no interaction with up to half of their friends. So, a new *interaction graph* is proposed to reflect the real user interactions in social networks, where only visible interaction between two users can create an edge in the graph, instead of being friends only. The article demonstrates that using an interaction graph performs better than using a friendship graph.

3. MOBILE SOCIAL BEHAVIOR

Nowadays, peoples can access social networks using their mobile phones. One can access social networks regardless of time and location. Major OSN platforms such as Facebook, Twitter, and LinkedIn release mobile applications to allow users to access their services through mobile devices. On the other hand, more mobile-centric functions have been integrated into OSNs, such as location based services and mobile communication. Understanding the user behavior in MSNs is very helpful for the design and implementation of MSN systems, improving the system efficiency in mobile environments or supporting better mobile-centric functions. In this section, we focus on studies of user behaviors in MSNs.

3.1 EXISTING SOLUTIONS

3.1.1 SOCIAL SERENDIPITY:

There are a large number of useful mobile social applications. *Social Serendipity* [6] is a mobile-phone-based application. In simple words it is mobilizing social software. It combines widely used mobile phones with the functionality face-to-face interactions between nearby users who do not know each other but probably should. Using Bluetooth, Serendipity senses nearby people and utilizes a centralized server to decide whether two users should be introduced to each other.

The system extracts common features between two user's profile and behavioral data. Then this information is summed according to user defined weights and a similarity score is created. A threshold will be already set by two users and if this score is greater than the threshold, then the system sends information to both users that someone might be interested in you. This application is used in large companies to introduce people working on same project. It is emphasized that privacy issues are important and fundamental in Serendipity, and privacy-protecting tools should be designed carefully.

3.1.2 ROUTING IN DELAY TOLERANT NETWORKS

This section seeks to understand human mobility in terms of social structures. Social structures are used in the design of forwarding algorithms for Pocket Switched Networks (PSNs). Many MANET and some DTN routing algorithms [7] [8] provide forwarding by building routing tables whenever mobility occurs. But in the case of PSN's where mobility is unpredictable, this routing method seems to be in efficient and not cost effective. Due to the mobility of devices, PSNs are intermittently connected, and effective routing protocols are essential in such networks. So social networks are preferred which are less volatile than mobility. *BUBBLE Rap* [9] is a social-based forwarding method which can be used for PSNs. Two social and structural metrics, centrality and community, are used to effectively enhance delivery performance. In this application, mobile users subscribe to a dynamic-content distribution service, offered by their service provider. A user community receives frequent updates from a common service provider. Here subscribers share their updates in an opportunistic fashion. These opportunistic exchanges can be used to extend the network's coverage and improve network efficiency. As shown in Fig. 1, BUBBLE Rap first uses a centrality metric to spread out the messages to more popular nodes and then uses a community metric to identify the destination community and deliver the messages to the destination.

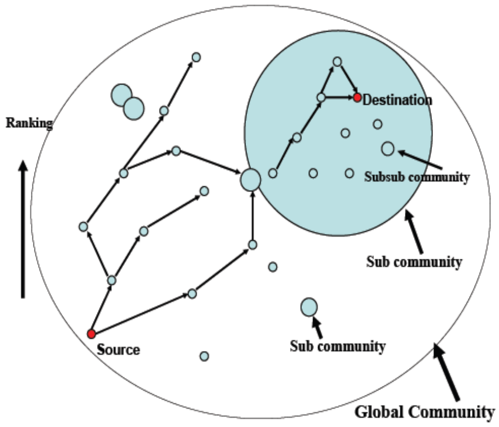

Fig 1: Illustration of BUBBLE Rap algorithm

3.1.3 LOCATION BASED SOCIAL NETWORKS

Although human movement and mobility patterns have a high degree of freedom and variation, at a global scale human mobility exhibits structural patterns subject to geographic and social constraints. One would expect that people exhibit strong periodic behavior in their movement as they move back and forth between their homes and workplaces .Cho *et al.* [10] aim to understand the basic laws that govern human motion and dynamics, using cell phone location data, as well as data from two online locations based social networks. It is found that humans experience a combination of strong short-range spatially and temporally periodic movement that is not impacted by the social network structure, while long-distance travel is more influenced by the social network ties. The article has shown that social relationships can explain about 10 to 30 percent of all human movement, while periodic behavior explains 50 to 70 percent. Cho *et al* studied the relation between human geographic movement, its temporal dynamics, and the ties of the social network. The role of geography and daily routine on human mobility patterns as well as the effect of social ties, i.e., friends that one travels to meet were analyzed. Based on the findings, a model of human mobility is proposed that combines periodic short-range movements with travel due to the social network structure and gives an order of magnitude better performance than previous models.

3.1.4 IMPROVING LOCATION PREDICTION

Nowadays people spent more time in online. So the data regarding geography and social relationships are increasingly precise. While we would like to believe that our social options are endless, human relationships are constrained in many ways. All of these constraints create a predictable structure where geography, transportation, employment, and existing relationships predict the set of people with whom we will associate and communicate. Using user supplied address data and the network of associations between members of the social network; one can directly observe and measure the relationship between geography and friendship. In [11], the study of user-contributed address and association data from Facebook shows that the addition of social information to the task of predicting physical location produces measurable improvement in accuracy when compared to standard IP-based methods. First, friendship is represented as a function of distance and analyzed the rank and generated observations regarding the interplay of geography and friendship. The observations were

- At medium to long-range distances, the P (friendship) is roughly proportional to the inverse of distance.
- At shorter ranges, distance does not play as large of a role in the likelihood of friendship

Using a maximum likelihood approach, they were able to guess the physical location of 69:1% of users with 16 or more located friends to within 25 miles, compared to only 57:2% using IP-based methods.

3.1.5 OPTIMAL AND SCALABLE CONTENT DISTRIBUTION

Ioannidis *et al.* [12] study the dissemination of dynamic content, such as news and traffic information, over an MSN. In this application, mobile users subscribe to a dynamic content distribution service offered by their service provider. To improve coverage and increase capacity, it is assumed that users share any content updates they receive with other users they meet. Reference 12 determines how the service provider can allocate its bandwidth optimally to make the content at users as "fresh" as possible. Even if the total bandwidth dedicated by the service provider remains fixed, the expected content age at each user grows slowly (as log(n)) with the number of users n.

4. TRAFFIC IN OSN

As company intranets continue to grow it is increasingly important that network administrators are aware of the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve problems when they occur, so as to not bring network services to a stand still for some periods of time. Social graphs of these social networks reveals about the connection and interaction of users in these OSNs. But that information provided are limited because various types of activities of users cannot be characterized. For example, how long a user browses a profile or how many posts a user has viewed are not characterized. These observations interpret how an user uses the OSN. It is important for Internet Service Providers to have better understanding of traffic pattern between end users and OSN sites. So ISP could take optimization actions according to the distribution and activities of OSN users. In this section, a review on OSN user behavior study from the perspective of network traffic analysis is done.

4.1 EXISTING SOLUTIONS

4.1.1 TRAFFIC MONITORING

Traffic monitoring is an efficient method of studying OSN. Crawling social networks provides us some limited information. Besides crawling, OSNs can also be studied by monitoring the network traffic. Benevenuto *et al.* [13] analyze the user behavior of OSNs based on clickstream data collected over 12 days with HTTP sessions of 37,024 users who used popular social networks of the time like Orkut, MySpace, Hi5, and LinkedIn. The data were collected from a social network aggregator website as in Fig 2, which enables users to connect to multiple social networks with a single authentication. This analysis revealed how frequently people connect to social networks and for how long, as well as the sequences of activities that users conduct on these sites.

Using clickstream data, patterns in social network workloads and social interactions were identified. The article also showed that the clickstream data provided information on silent interactions.

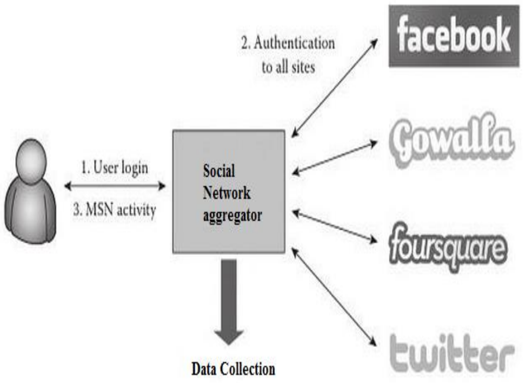

Fig 2: Data collection through a social network aggregator. [2]

This article defines and analyzes the OSN session characteristics:

- The frequency at which OSNs are accessed
- Total time spent on OSNs
- Session duration of OSNs

Schneider *et al.* [14] also study clickstream data, but their focuses are feature popularity, session characteristics, and the dynamics within OSN sessions. They made research for the answers of

- Which features of OSNs are popular and capture the users' attention?
- What is the impact of OSNs on the network?
- What needs to be considered when designing future OSNs?
- Is the user's behavior homogeneous?

HTTP request-response pairs show the popularity of different features. The popularity of features can be different based on location of user, type of OSN and time spent by the user. Besides, the distribution of transmission bytes per OSN session is given, which helps the ISPs learn the traffic pattern of different OSNs.

The article presented a customizable methodology to identify OSN sessions and user actions within the OSN. The methodology enabled to extract OSN usage information across a wide range of features, from coarse information like session duration to minute details about the kinds of profiles the user accesses. The distribution also shows the duration of sessions and number of sub sessions within a session. Moreover, the article reveals the dynamics within OSN sessions. It is found that users can be inactive when accessing the OSNs.

Clickstream data can be incomplete, which restricts its usage and performance. Click-stream data is limited by the collection duration and monitoring locations and the behavior of inactive users in the duration is not monitored. That is, only the behavior of users using certain monitored ISPs is captured.

4.1.2 NAVIGATION CHARACTERISTICS

Online social networks (OSNs) represent a significant portion of Web traffic today. OSNs are impacting how users navigate the Web and the types of websites they visit. Dunn *et al.*[15] try to study visit of website users through OSNs vs. through search engines. Using web traffic logs from 17,000 digital subscriber line (DSL) subscribers of a Tier 1 ISP in the United States, it is found that OSN visitors are less likely to navigate to external web sites. But when they visit external web sites, OSN users will spend more time at those web sites compared to search.

4.1.2 LOCALITY OF INTEREST

An integral part of the success of OSN is the immense size of their global user base. If we use Facebook as our user case, to provide a consistent service to all users, Facebook is heavily dependent on centralized U.S. data centers and wasteful of Internet bandwidth. As a result, users outside the United States experience slow response time. Also, a lot of unnecessary traffic is generated on the Internet backbone. Wittie *et al.* [16] investigate the detailed causes of these two problems and identify mitigation opportunities. It is found that OSN state is amenable to partitioning. The fine-grained distribution and processing of OSN can significantly improve performance without loss in service consistency.

Based on simulations of reconstructed Facebook traffic over measured Internet paths, it is shown that user requests can be processed 79 percent faster and use 91 percent less bandwidth. Therefore, the partitioning of OSN state is an attractive scaling strategy for OSN service providers.

5. SOCIAL TAGGING BEHAVIOR

Nowadays webs are so open that it makes easier for end users to join social networks. [26] Shows that social networks have pioneered online communities, allowing users to contribute to collective knowledge by tagging online resources. Tagging behavior increased a lot between 2005 and 2012. Joao Paulo Pesce et all [27] demonstrates how the simple act of tagging pictures on the social-networking site of Facebook could reveal private user attributes that are extremely sensitive. The results suggest that photo tags helps in predicting some, but not all analyzed attributes.

6. MALICIOUS BEHAVIOR

In this section, an initial study to quantify and characterize malicious attacks launched on Online Social Networks is performed. Unfortunately, recent evidence shows that these communities can become effective mechanisms for spreading malware and other malicious attacks.

The usage of OSNs introduces numerous security and privacy threats. Popular OSNs are increasingly attacked from large botnets. Using compromised or fake accounts, attackers can turn the trusted OSN environment against its users by miss spreading spam messages as communications from friends and family members. Also data (photos, article, private messages, etc.) may be leaked to a third party without the user's explicit authorization, even when the user regards them as confidential. Sybil attacks are also common in OSNs.

6.1 EXISTING SOLUTIONS

6.1.1 SPAM CAMPAIGNS

OSNs become effective tools for executing spam campaigns and spreading malware. A user is more likely to respond to a message from a friend than from a stranger. Thus social spamming is a more effective distribution mechanism than traditional email. Gao *et al.* [17] study a large dataset composed of over 187 million wall messages among 3.5 million Facebook users. The system detected 200,000 malicious wall posts with embedded URLs originating from more than 57,000 accounts. It was discovered that more than 70 percent of all malicious wall posts advertise phishing sites. It is also found that more than 97 percent are compromised accounts rather than "fake" accounts created solely for the purpose of spamming. Finally, spamming dominates actual wall post activity in the early morning hours, when normal users are asleep.

6.1.2 DETECTION OF FAKE ACCOUNTS

Spam is common across many types of electronic communication, including email and social networks. To increase financial gain and also to reach more users many spammers now use multiple content sharing platforms including online social networks to disseminate spam. Q.Cao *et al.*[24] proposed SybilRank, an effective and efficient fake account inference scheme, which allows OSNs to rank accounts according to their perceived likelihood of being fake.

OSNs suffer from abuse in the form of the creation of fake accounts, which do not correspond to real humans. Lumezanu *et al.* [18] performed a joint analysis of spam in email by taking Yahoo mail as user case and social networks by taking Twitter as user case. It was observed that email spammers that also advertise on Twitter tend to send more email spam than those advertising exclusively through email. Furthermore, sending spam on both email and Twitter has better exposure than spamming exclusively with email.

6.1.3 ANONIMITY

Social Networks are intermediate between being monolithic proprietary applications and open applications in the federated identity management space. ENISA's position paper [19] pointed out that the tendency towards a lock-in effect inherent in Social Networking revenue models was detrimental to user privacy and security. ENISA recommended that open formats and standards should be developed to break the data lock-in effect and counterbalance this economic and social pressure.

In [20] social key-trust, a public key is used to encrypt social data. Such a scheme could also be used as a basis for a smart way of encrypting data in social networks to strengthen privacy so that network members with an adequate trust level in their keys. Possibly even the service provider cannot see the data.

6.1.4 SYBIL DEFENSE

Avoiding Sybil attacks also known as multiple identities is known to be a fundamental problem in the design of distributed systems [25]. Malicious attackers can create multiple identities and trouble the working of systems that rely upon open membership. Sybil attacks are the fundamental problem in peer-to peer systems and other distributed systems. Recently, a number of social network-based schemes, such as *SybilGuard*, *Sybillimit*, *SybilInfer*, and *SumUp*, have been proposed to eradicate Sybil attacks.

Viswanath *et al.* [21] studied on these Sybil defense schemes and shows that existing Sybil defense schemes work by identifying local communities around a trusted node. So it is needed to design general community detection algorithm. Manual inspection needs to be involved in the decision process for suspending an account. *Sybil Rank* [22] aims to efficiently derive a Sybil-likelihood ranking and only the most suspicious accounts need to be inspected manually. It is based on efficiently computable early-terminated RWs and is suitable for parallel implementation on a framework such as Map Reduce, uncovering Sybils in OSNs with millions of accounts. Sybil Rank is deployed and tested in the operation center of Tuenti, which is the largest OSN in Spain with 11 million users.

7. FUTURE WORK

The First section states that the dynamic feature is an important aspect to deeply understand an OSN's user behavior. Existing method used static way of investigation. Considering this dynamic can extract more inherent information than studying static data. This helps in revealing present situation and also predicting some future activities. Also, studying different time intervals and time granularities would lead to more interesting findings. For dynamic analysis an unbiased and efficient graph sampling algorithm can play an important role. These algorithms can result in fast data collection and timely processing. Information storage is another challenge while collecting dynamic data. So, the temporal and spatial dependence between different data items can be utilized for better compression.

The second section reveals that future research work is needed in MSNs in privacy, energy efficiency ,content distribution, community detection, protocol sharing. Algorithms should be designed for precise localization. Continuous exploration is needed in the area of incentive mechanism, identity management, trust, reputation, methods for social network metrics estimation. A comprehensive summary related to applications, architectures, and protocol design issues for MSNs can be found in [23].Services should be improved to meet demand for social activities in cyberspace .Work should be expanded in data analyzing, modeling, and prototyping.

The third section shows us that most analysis performed by ISPs is without the active involvement of OSN service providers which limits the range of study. Not all crawling data are available to ISP because of restrictions provided by service provider. Although an ISP is able to capture and analyze all its traffic to/from an OSN site through traffic monitoring, it can only get a partial view. Only users who get access to OSNs through a specific ISP's infrastructure can be observed. Study on user behavior can enhance the user experience interactively and quickly. Also, this will save operational costs for OSN providers. The fourth section shows that exploring relative popularity of tagging feature by the users for OSN sessions need further research.

From the fifth section, it is understood that OSN suffer from the problem of privacy breach. To maintain privacy decentralized OSN is a good measure but switching of users to a decentralized OSN is a challenge. Further the recipient of shared information should be controlled by user itself. Sybil defense is an interesting topic where researches are going on.

8. CONCLUSION

This paper studied user behavior of OSN from five perspectives. This study provided insight into human social behavior to some extent. The paper reviewed the solutions existing currently for the challenges in online social networks and made a study on future challenges to be solved. This research will improve user experience and satisfy Internet service providers, OSN controllers and end users. I believe that further study on this topic generate more research problems and suitable solutions in the area of Online Social Networks.

REFERENCES

[1] Orkut Help. http://www.google.com/support/orkut/.

[2] M.Gjoka *et al*, “Practical Recommendations on Crawling Online Social Networks,” *IEEE Trans. Common.* Special Issue on Measurement of Internet Topologies, vol.29, no. 9, Oct. 2011.

[3] J.Jiang *et al.*, “Understanding Latent Interactions in Online Social Networks,” *Proc. IMC*, 2010.

[4] H. Kwak *et al.*, “What Is Twitter, a Social Network or a News Media?” *Proc. WWW*, 2010.

[5] C. Wilson *et al.*, “User Interactions in Social Networks and Their Implications,” *Proc. EuroSys*, 2009.

[6] N. Eagle and A. Pentland, “Social Serendipity: Mobilizing Social Software,” *IEEE Pervasive Computin*g, vol. 4, no. 2, 2005, pp. 2834.

[7] E. P. C. Jones, L. Li, and P. A. S. Ward, “Practical routing in delay tolerant networks,” *In Proc. WDTN, 2005.*

[8] Lindgren, A. Doria, et al. Probabilistic routing in intermittently connected networks. *In Proc. SAPIR, 2004.*

[9] P. Hui, J. Crowcroft, and E. Yoneki, “BUBBLE Rap: Social Based Forwarding in Delay Tolerant Networks,” *IEEE Trans.Mobile Computing*, vol. 10, Nov. 2011, pp. 1576–89.

[10] E. Cho, S. Myers, and J. Leskovec, “Friendship and Mobility: User Movement in Location-Based Social Networks,” *Proc. KDD*, 2011.

[11] L. Backstrom, E. Sun, and C. Marlow, “Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity,” *Proc. WWW*, 2010.

[12] S. Ioannidis, A. Chaintreau, and L. Massoulie, “Optimal and Scalable Distribution of Content Updates over a Mobile Social Network,” *Proc. INFOCOM*, 2009.

[13] F.Benevenuto *et al.*, “Characterizing User Behavior in Online Social Networks,” *Proc. IMC*, 2009.

[14] F.Schneider *et al.*, “Understanding Online Social Network Usage from a Network Perspective,” *Proc. IMC*, 2009.

[15] C. W. Dunn *et al.*, “Navigation Characteristics of Online Social Networks and Search Engines Users,” *Proc.WOSN*, 2012.

[16] M. Wittie *et al.*, “Exploiting Locality of Interest in Online Social Networks”, *Proc. Co Next*, 2010.

[17] H. Gao *et al.*, “Detecting and Characterizing Social Spam Campaigns,” *Proc. IMC*, 2010.

[18] C. Lumezanu and N. Lumezanu, “Observing Common Spam in Tweets and Email,” *Proc. IMC*, 2012.

[19] ENISA**.** Security Issues and Recommendations for Online Social Networks. [Online] 2007. http://www.enisa.europa.eu/doc/ pdf/ deliverables /enisa _pp _social_networks.pdf.

[20] Giles Hogben, “*ENISA Position Paper for W3C Workshop on the Future of Social Networking* “2011.

[21] B. Viswanath *et al.*, “An Analysis of Social Network Based Sybil Defenses,” *Proc. SIGCOMM*, 2010.

[22] H. Gao *et al.*, “Security Issues in Online Social Networks,”*IEEE Internet Computing*, vol. 15, no. 4, 2011.

[23] N. Kayastha *et al.*, “Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey,” *Proc. IEEE*, vol. 99, no. 12, 2011, pp. 2130–58.

[24] Q. Cao *et al.*, “Aiding the Detection of Fake Accounts in Large-Scale Online Social Services,” *Proc. NSDI*, 2012.

[25] J. Douceur *et al*,”The Sybil Attack”, In Proc. IPTPS’02, Cambridge, MA, Mar, 2002.

[26] Ying Ding *et al*.,” Profiling Social Networks, A Social Tagging Perspective”, D-Lib Magazine, March/April, 2009.

[27] Joao Paulo Pesce et all,” Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook”, april 2010.