

Communities Against Deception in Online Social Networks

Sajid Yousuf Bhat & Muhammad Abulaish, *SMIEEE*

Department of Computer Science, Jamia Millia Islamia (A Central University)

Jamia Nagar, New Delhi - 110025, India

Email: s.yousuf.jmi@gmail.com, mAbulaish@jmi.ac.in

Short Abstract:

The high popularity and membership of online social networks has also attracted deceptive malicious activities which mainly target the privacy and security of its users and their identities. It is now considered a big challenge to devise novel approaches which can identify the stealthy accounts that launch such attacks on legitimate users in online social networks.

Long Abstract:

Malicious activities in online social networks (OSNs) have transformed from simple forms of spamming to highly deceptive forms including Sybil attacks and Cloning attacks both of which are primarily focused on breaching the privacy of online social network users and ultimately their trust. Traditional content-based and collaborative filtering techniques seem to give average performance in identifying the fake accounts used to drive these attacks. Topological characteristics of legitimate users like the formation of tightly knit communities amongst them can be seen as potential basis for categorizing legitimate and fake accounts in OSNs. However, the task becomes challenging due to the observations which indicate that malicious accounts attempt to mimic some topological characteristics like the formation of interconnected groups. It is thus a highly desirable task to devise efficient techniques and methods for identifying spammers, Sybils and Clones in OSNs.

1 The Platform

Online social networking sites (OSNs) like Facebook and Twitter have become highly popular on the internet with millions of members where they share information and content, and connect with each other. The connections thus established highly reflect the real-world relationships between the users of these social networks. These sites are being looked upon as high-potential marketing opportunities by many organizations for the purpose of popularizing their products. OSNs offer many useful properties that reflect real-world social network characteristics, which include small-world behavior, significant local clustering, existence of large strongly connected component and formation of tightly knit groups or communities [1][2][3].

The wide popularity of OSNs and their ease of access has also resulted in the misuse of their services. Besides the issue of preserving user privacy, OSNs face the challenge of dealing with deceptive users and their malicious activities in the social network. The most common form of malicious activity identified in OSNs is spamming which involves malicious users to broadcast irrelevant information in the form of messages and posts to as large number of legitimate users as possible. Spamming is done mostly with an aim of promoting products, viral marketing, spreading fads, and in some cases may possibly be done to harass legitimate users

of an OSN in order to decrease their trust in the particular service. Unlike traditional e-mail networks, wherein content based filtering of e-mail messages has proved promising to identify spammers, deception in online social networks has take a step forward. Filtering of undesirable accounts in OSNs is often faced with challenges like the existence of a thin line between the content shared by legitimate users and malicious accounts. Moreover, the deceptive accounts often tend to mimic the behavior of legitimate users, making it difficult to detect and categorize them. Two highly deceptive malicious activities that have been recently identified include the Sybil attack and the Cloning attack [4][5]. On the OSNs a Sybil attack in its basic form involves a single attacker to create groups of malicious accounts which intend to deceive the system by forming communities to appear as legitimate nodes and disseminate spam to the legitimate parts of the network by deceiving legitimate users in creating trusted links with them, thus breaching their privacy. With the similar intentions of breaching user privacy in online social networks, deception in the form of a Cloning attack involves copying the profile details of a legitimate user to form a fake account and then breach the trust the friends of the legitimate user with malicious intentions.

One of the distinct feature of OSNs, from traditional e-mail networks, is that OSN interactions are limited within a particular service. For example, only Facebook users can interact with other Facebook users while as e-mails transfers can occur across services. This feature gives a centralized control over the accounts' behaviors in a particular OSN and a centralized deception defense system can be implemented and evaluated to counter malicious activities within that social networking service. Existing spam/spammer detection methods are mostly based on the content analysis (keywords-based filtering) of the interactions between users. However, many counter-filtering techniques based on the usage of non-dictionary words and images in spam objects are often employed by spammers. Content-based spam filtering systems also demand higher computations. Moreover, the issue of privacy-preservance of user content (private messages, posts, profile details) is often held against content-based spam filtering systems. Alternatively, some spammer detection techniques are based on learning classification models from network-based topological features of the interacting nodes in online social networks. These features mainly include in-degree, out-degree, reciprocity, clustering coefficient, etc.

2 The Mischief

In traditional e-mail networks, the most common form of spamming involves the Random Link Attack (RLA) where a small number of spammers send spam to a large number of randomly selected victim nodes. Spammers tend to be senders of spam messages to a socially un-related set of receivers, unlike legitimate senders whose receivers tend to cluster or form communities as discussed earlier[6]. It is unlikely that the recipients of the spam messages sent by a spammer have friend or friend-of-friend relations or have some kind of mutual ties among them [7]. As a result, a distinctive feature that has often been used to detect spammers is the clustering coefficient (CC) by considering that networks representing connections of legitimate users show high CC while spammers show CC close to 0 [8]. However, in case of OSNs, deceptive spammers attempt to make their neighborhood structurally similar to legitimate nodes and thus increase their CC, making it hard to detect them. Such a collaborative attack is termed as a Sybil attack and involves connected groups of Sybil accounts (mimicking clustering behavior of legitimate users) spam or influence legitimate users as shown in figure 1.

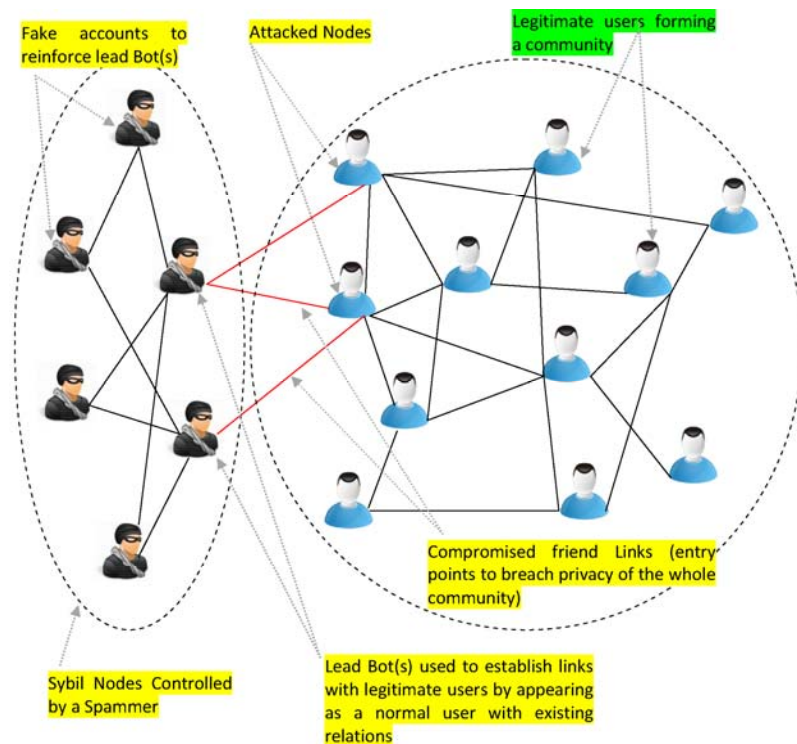
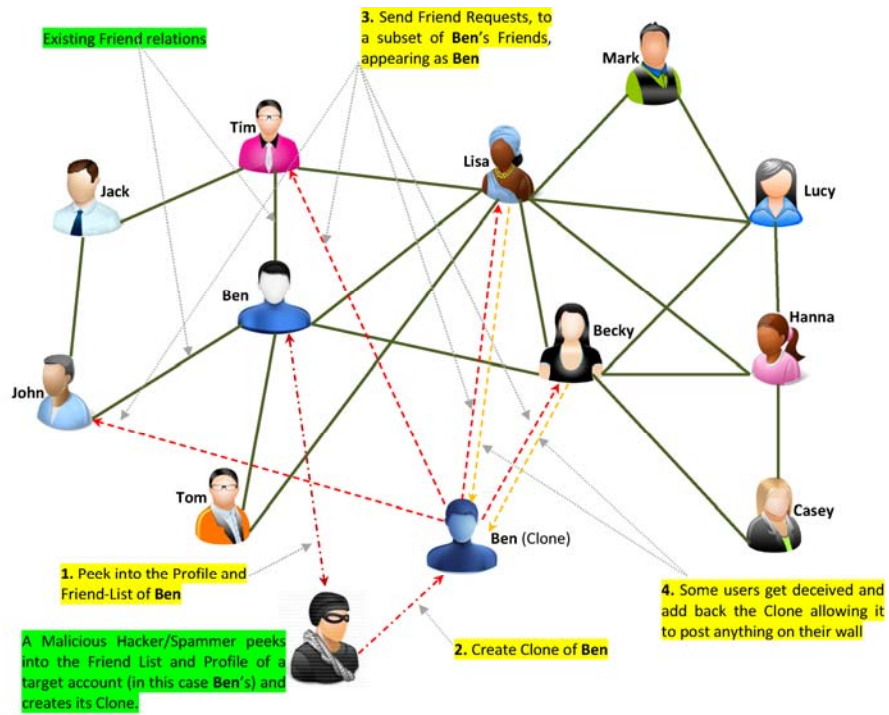
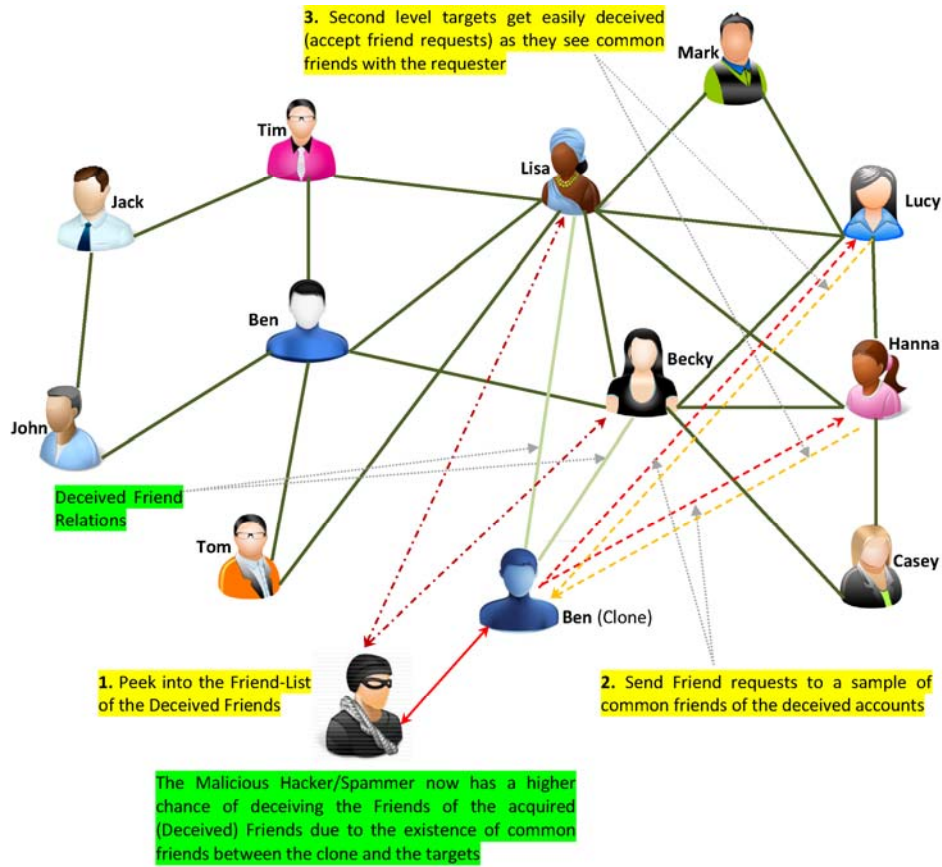


Figure 1: A sybil attack

Another detection scheme that is commonly used to stop spam and identify spammers based on collaborative filtering involves using a user voting scheme to classify a message as spam or non-spam. The message recipients are provided with options by their messaging service providers to vote a received message as spam or non-spam. These votes are then collectively used to identify spamming IP addresses and user accounts [9]. However, a deceptive scheme used by spammers to get away from collaborative filtering spam detection methods is the vote-gaming attack wherein, spammers add some of the secondary accounts (Sybils) controlled by them to the recipients list of spam messages sent from a spamming account. When a secondary account receives a spam message that is already classified as spam, the bot controlling the secondary account reports the message as non-spam. Considering non-spam votes from multiple secondary spammer accounts, the spam filtering system notices the lack of consensus and does not filter the message as spam for other recipients. Analogously, in case of OSNs such a voting game is often played by Sybil accounts to assign higher rating (likes in case of Facebook and followers in case of Twitter) to some particular Sybil account(s) or the content generated by them.



(a)



(b)

Figure 2: Illustration of a cloning attack in two stages

Similar to coordinated Sybil attacks, deception in online social networks has also taken the form of cloning (copy profiling). It mainly involves an attacker to extract information related to the profile details and friend relations of a target user (including profile picture(s)). Based on this extracted information, the attacker creates an exact profile (clone) as that of target and sends friend requests to a subset of friends of the target. On receiving the friend requests from the clone, some non-suspicious or less active recipients may falsely consider the requests to be coming from the actual target user and as a result add back the clone without realizing the fact that the same/similar profile already exists in their friend list. This first stage/level is very crucial for an attacker, i.e., if it is successful in befriending some legitimate user(s) initially then it has a higher chance of breaching the social circle and trust of the other legitimate users, which now have common friends with the clone, in the second and later stages. A clone attack in its two stage form is illustrated in figure 2 wherein figure 2a shows the first stage of an attacker cloning a legitimate user (Ben) and multicasting friend requests to a subset Ben's friends, out of which a few accept. Similarly, figure 2b shows how the attacker, in the second stage, samples accounts with which it has common friends to repeat the infiltration process. An advanced cloning attack may even involve creating multiple clones (of different accounts) at various stages of infiltrations to remain stealthy and maximize its reach. After breaching the social circles of the legitimate users through cloning, an attacker has a lot of options for exploiting the legitimate users under its reach. It may involve posting spam directly on the walls of legitimate users, launching phishing attacks based on trust relations, inducing buying behavior and even controlling online protest campaigns.

One of the unique distinguishing properties between spammers and normal users in OSNs is that the interactions of spammers are least often reciprocated while as, mostly, all of the legitimate user interactions are reciprocated. Moreover, the reciprocated interaction average of spammers is close to zero as most of the spam are simply ignored or discarded by recipients. It may also be the case that a group of coordinating sybil accounts of a spammer fake communication reciprocity between them by reciprocating each other's interactions which they also send as spam to a comparably small set of legitimate targets so as to increase their reciprocated interaction average. However, in order to be effective as spammers and meet their goals, they need to target a larger number of legitimate nodes as possible. Spamming a small number of legitimate nodes in the system will have a negligible effect on the system. It means that faking interaction reciprocity alone is not a good solution for spammers to deceive a filtering system which considers the interaction reciprocity for detecting spammers.

3 The Defence

Most of the techniques and methods developed for spammer or spam detection from online social networks involve a content based approach. Such approaches learn classification models using various machine learning techniques from known spam instances (training set) based on the textual features of spammer profile details (about me, address and so on) or their interactions (e-mails, messages, wall posts and so on) or both. The main idea is based around the observation that spammers use distinguished keywords, URLs and so on in their interactions and to define their profiles. However, it is not always true and such an assumption is often deceived by the approaches like copy-profiling and content obfuscation. In order to improve spam/spammer detection, besides textual-features, additional features based on images, topological properties of interaction networks and social network properties have

recently been used. Lee et al. define social honeypots (administered bot accounts) that monitor spammers' behaviors and log their information [10]. If the social honeypot detects suspicious user activity (e.g., the honeypot's profile receives a friend request, message, wall post and so on) then the social honeypot's bot collects evidence of the spam candidate. They further use machine learning techniques to learn classification models from the information collected by the social honeypots. However, one of the main limitations of social honeypots is their reach, i.e., not all spammers would target them, and that the classifiers can possibly be deceived if the spammers involve a clone attack. As mentioned earlier, the issues related to user-privacy and computational requirements of content based filtering systems often hints on using only link based, topological and social network properties of the communication networks for identifying spammers. To detect spam clusters, Gao et al. use two widely acknowledged distinguishing features of spam campaigns: their "distributed" coverage and "bursty" nature [11]. The "distributed" property is quantified using the number of users that send wall posts in the cluster. The "bursty" property is based on the intuition that most spam campaigns involve coordinated action by many accounts within short periods of time. Moreover, communication reciprocity, communication interaction average and clustering coefficient of the nodes in OSNs have also been used to differentiate spammers from legitimate users. Existing graph-based Sybil detection methods are based on the assumption that the Sybils cannot form random links with many legitimate users and the legitimate users tend to form tightly knit communities rapidly.

4 The Community Shield

A community based defense system aims to detect the communities of spammers doing a random link attacks or coordinated Sybil attack in online social networks. The community based spammer detection approach discussed here is inline but better than Fire et al. wherein they use a community detection method to split the interaction network into communities. Then extract features based on the degree of a user, the number of communities the user is connected to, number of links between the friends of the user, and the average number of friends inside each of the user's connected communities [12]. The approach presented here also builds upon the observations made by Viswanath et al. which indicate that explicit community detection algorithms can be used to defend against Sybils in online social networks [13]. It is based on learning a classification model from community-based features of the nodes after identifying their node level community structure from the weighted interaction graph of the social network. The weight of a directed link in the graph represents the total number of messages, posts, etc., sent from the origin to the destination. The basic idea of the approach is shown in figure 3, and the various steps involved in the process are discussed in the following sub-sections.

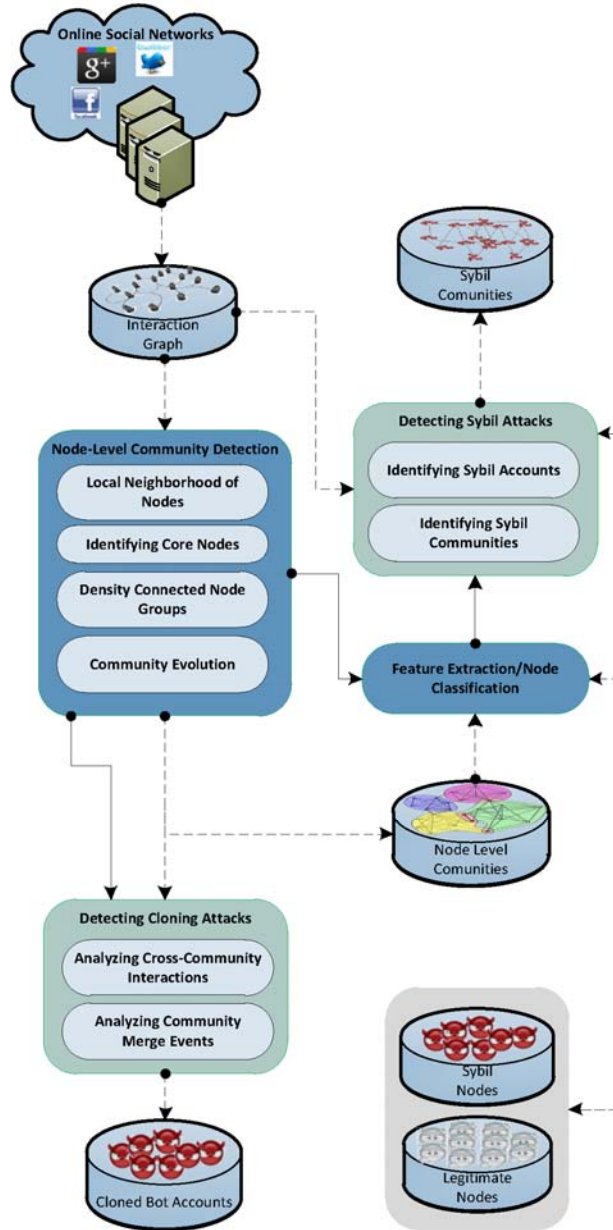


Figure 3: Overview of the community-based shield framework

4.1 Node Level Community Detection

The framework starts with detecting density-based node level overlapping communities from the interaction graph of online social network users using the OCTracker algorithm [14]. Some of the important features of this method include, a) categorizing nodes as cores (important nodes in a community), non-cores (boundary nodes of a community), and outliers (nodes which do not belong to a community), and b) Overlapping nature of nodes, i.e., the number of communities a node assigned to. The interaction graph on which the community-detection method is applied is usually generated from the activity logs of the users like the wall-post logs, timelines and so on.

4.2 Features

Once the overlapping community structure of nodes is identified the next step involves extracting community-based and some topological features of nodes in the network. They include the features which express the role of a node in the community structure, i.e., whether a node is a boundary node or a core node and the number of communities it belongs to (if any). It also uses out-degree and reciprocity related node features, however, in the light of community membership. The various features and their description are given as follows:

Total out-degree: The total out-degree of a node represents the total number of distinct users in the social network to which it has out links, i.e., sends messages etc.

Total reciprocity: The total reciprocity of a node represents the ratio of the number of nodes with which it has both in-links and out-links, to the total number of nodes to which it has out-links.

Total in/out ratio: For a node p it represents the ratio of the number of nodes which have out-links to p to the number of nodes and to which node p has out-links,

Core node: This is a boolean property which is true for a node p if the community detection method used here, OCTracker, marks the node p as a core-node, otherwise it is false.

Community memberships: This feature represents the number of communities to which the overlapping community detection method, OCTracker, assigns a particular node p . For the outlier nodes, the value for this feature will be zero.

Foreign out-degree: The total number of foreign nodes (*for a node p , a node q is called a foreign node if the two nodes p and q do not belong to a common community*) to which a node p has out-links is called the foreign out-degree of node p .

Foreign in/out ratio: The foreign in/out ratio for a node p is defined as the ratio of the number of foreign nodes that have out-links to the node p to the number of foreign nodes to which node p has out-links.

Foreign out-link probability: This feature represents the probability that a particular node p has an out-link to a foreign node.

Foreign reciprocity: For a node p the foreign reciprocity is the amount of reciprocated interactions (response) shown by the foreign nodes to the interactions of p .

Foreign out-link grouping: This feature basically represents the probability that the foreign nodes to which a node p has out-links have a common community.

4.3 Classification

Based on the extracted node features, a classifier is learnt using a set of pre-labeled nodes in the interaction graph that have already been classified as malicious or legitimate. These pre-labeled nodes can be the result of administrative filtering performed on the basis of either content filtering of profiles and messages, or user reports and feedback in online social networks. In either case, the community-based features of these pre-labeled nodes form the training set for learning the classifier. In literature, many machine learning methods have been used to learn classifiers based on topological and content-based features of spam and spammers in online social networks. The most commonly used classifiers include NaiveBayes, decision tree and k -NN to name a few. An illustration of the process of learning the classification model from the extracted features is presented in figure 4.

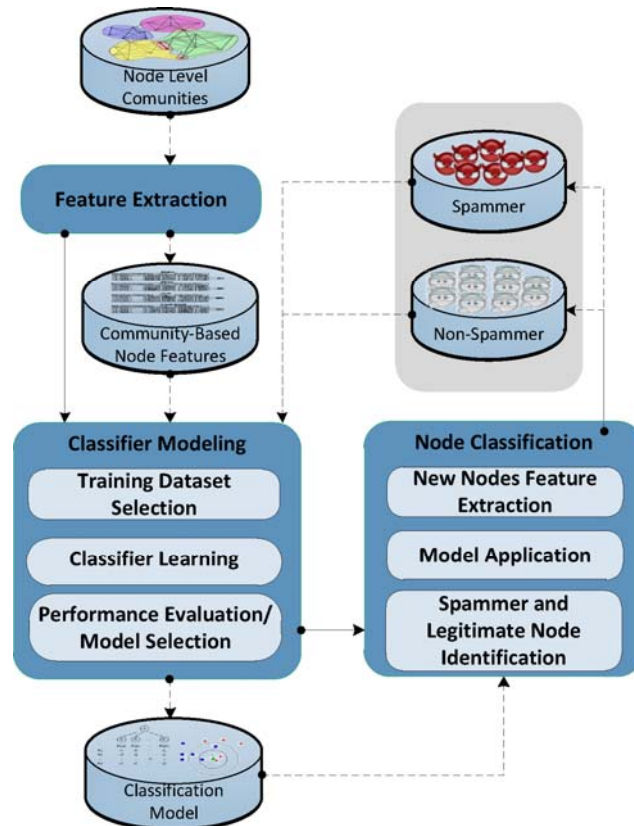


Figure 4: Classification model learning and application

The classification model selected from the learning phase is then used to classify un-labeled nodes of the interaction graph representing the online social network. The newly identified spammer nodes are reported to the system administrator who further decides whether to block the suspected nodes or completely remove them from the social network.

4.4 Finding Stealthy Sybils

Many spamming accounts, often controlled by a single malicious user, tend to mimic the clustering property of legitimate users and form Sybil communities. Sybil accounts and their communities are stealthy in the sense that they form links between themselves and also give an illusion of interactions between them making them look legitimate. A subset of accounts within a Sybil community are then used to lead an attack on the legitimate communities as illustrated in section 2. In order to identify these Sybil communities, The community shield builds upon the previous spammer classification scheme and the node level communities identified therein. The idea is that once nodes in an OSN are classified as spammers and legitimates by the classifier, the community membership of the identified spammers is examined and the node-level communities which tend to contain many spammers are labeled as Sybil communities. Moreover, the social network induced only by the spammer nodes can be extracted from the underlying online social networks based on interactions or friend relations. The resulting spammer network can be used to extract Sybil communities by applying the community detection algorithm on it.

5 A Case Study

The performance of the community shield based approach using some classification models including decision trees, NaiveBayes and k -NN implemented in the WEKA software [15]. A real-world social network with artificially planted spammer nodes is used for generating the results.

5.1 Dataset

A real-world datasets, representing the wall-post activity of about 32693 Facebook users is treated as a legitimate network. In order to simulate spammers, a set of 1000 isolated nodes is created with out-links to randomly selected nodes in the legitimate network (emulating a random link attack). The out-links or the out-degree generated for the spammers are not random but follow the distribution shown by real-spammers as shown in Table 1.

Table 1: Spammer out-degree distribution

y	P[out-degree=y]
1	0.664
2	0.171
3	0.07
4	0.04
5	0.024
6	0.014
7	0.01
8	0.007

The messages of the spammers are expected to be least often reciprocated. Thus the probability of a legitimate node replying to a spammer is set to 0.05. Besides emulating a random link attack, a Sybil attack on legitimate network is also created to make the detection task more difficult. A set of another 1000 spammer nodes which mimic the clustering/community property of legitimate nodes is created using a network generator. For each Sybil node a set of its out-links is rewired towards a set of randomly selected nodes in the legitimate network such that the spamming out-degree (i.e., the rewired out-links) follows the distribution given in Table 1. In this regard, a total of 2000 spammer nodes (out of which 1000 mimic the clustering property of legitimate nodes) are added to the legitimate network resulting in a total of 34693 nodes for the Facebook network. We now apply the overlapping community detection method OCTracker on the dataset and extract the various features for each node in the resulting networks.

5.2 Results

The performance of the community-based approach is measured by learning a set of classifiers from WEKA on the training examples containing the community-based features from the dataset mentioned in the previous section. A 10-fold cross validation is used for each classifier on the dataset to evaluate the performance. Figure 5 presents the performance of the various classifiers on the Facebook dataset with planted spammers. As can be seen from figure 5, the decision-tree based classifiers J48 and ADTree perform better than the others and have a low false-positive rate.

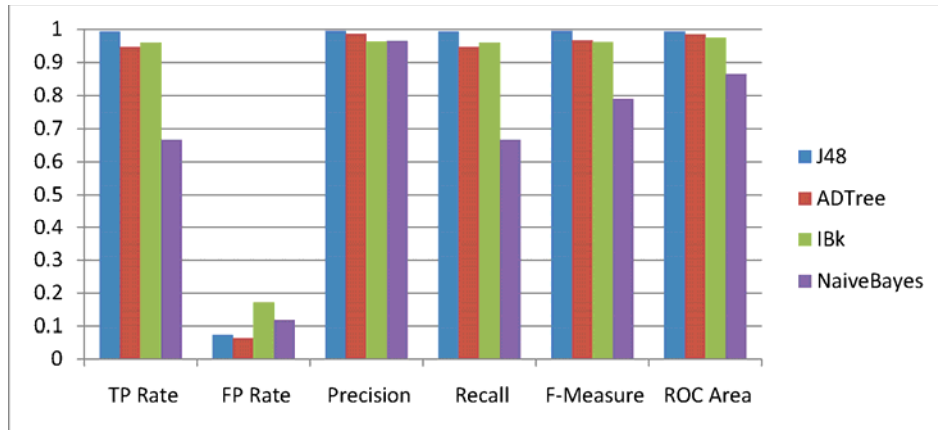


Figure 5: Performance on Facebook network with simulated spammers

In order to further ensure the significance of the various community-based features for identifying spammers in online social networks, the performance of J48 classifier using only the non-community based node features, i.e., out-degree, total reciprocity, and total in/out ratio is also presented as shown in figure 6. On comparing the results presented in figure 6 with the results of the J48 classifier in figure 5, it can be seen that using community based features of nodes in online social networks along with the non-community based features in classification shows better performance than simply using the non-community based features.

The preliminary results presented in this section indicate that the community-based approach to identify spammers from online social networks is promising as the classifiers learnt from the community-based features of OSN users show high accuracy for the task. Moreover, the proposed scheme directly identifies Sybil communities in the form of node level communities which have many nodes labeled as spammers. Similarly, the communities identified from the spammer induced network in the dataset also identify the same Sybil communities.

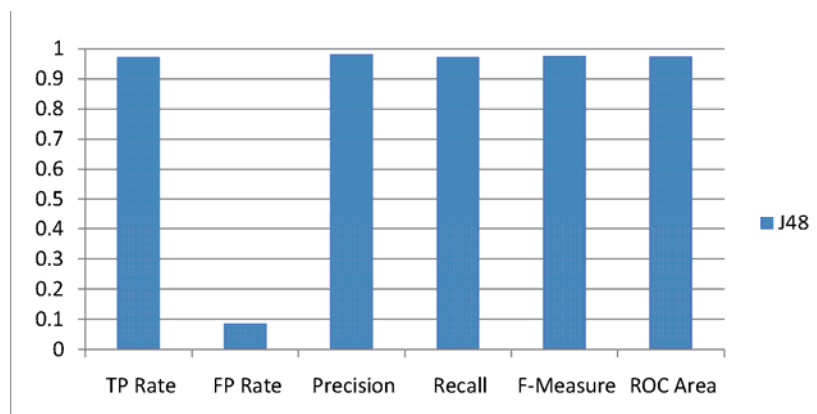


Figure 6: Performance of the J48 classifier using only non-community based features

6 Taming the Clone

The preliminary results indicated how spammers and Sybil communities can be identified using community based features from online social networks. However, unlike

spammers and Sybil attacks, cloning appears to be the most deceptive and successful form of malicious activity in online social networks and may often be difficult to track. An attacker driving a cloning attack follows a greedy approach with an aim of be-friending as many legitimate users, for each cloned account, as possible. However, the attacker ensures not to flood the neighborhood of a clone with friend requests and thus samples recipients from the friend list of a deceived legitimate account as illustrated in figure 2. Moreover, in order to avoid too many friend relations for a single clone, the attacker creates a new clone (of some newly crawled account) after some random length of the attack crawl and repeats the process. In order to increase the legitimate appearance of the clones, the attacker may also connect the clones in the same way as their actual images in the online social network.

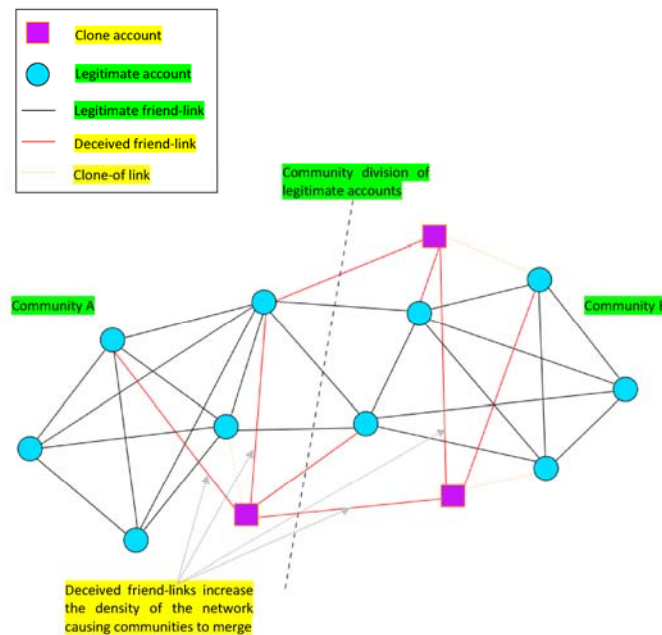


Figure 7: Illustration of tracking a cloning attack based on community-merge events

At this stage it can be argued that legitimate users tend to interact within their local communities and that the community evolutionary events including merge and split of communities in dynamic online social networks are not frequent and occur rarely as compared to events like the birth, death and growth of communities. On the other hand, the greedy behavior of the cloned accounts backed by an attacker tend to create more dense regions in the networks by adding more nodes and cross-links. This can cause adjacent communities to merge and may also trigger frequent community-merge events in the evolution of the network if the cloning attack is robust as demonstrated in figure 7. In this regard a community-tracking algorithm for dynamic networks like OCTracker can be used to track the community-merge events in the evolving friendship graph of an online social network and identify regions resulting in frequent merge events. These regions can be scanned for determining the level of *profile similarities* and *neighborhood overlap* between each pair of user-profiles having the minimum path length of 2 between them. Profiles with high similarity can be reported to an administrator and necessary steps taken to block the clone.

7 Conclusion

Online Social networking platforms are faced with numerous novel forms of malicious and deceptive attacks targeted over the trust and privacy of their users. Traditional content based approaches to identify spammers seem to lack an effective punch to take on the advanced stealthy tactics of the new age malicious accounts like Sybils and Clones. Considering topological features like those based on the community structure of the OSN users can better help in categorizing the behavior of malicious users from legitimate accounts. For example, analyzing the evolution of community structure of a dynamic friend network can identify Cloning attacks by tracking (frequent) community-merge events potentially caused by the interconnection of different legitimate communities through the Cloned accounts. It is thus the need of the hour to identify new approaches of tackling with malicious accounts using community based features of the OSN users.

References

- [1] L. A. Adamic and E. Adar, "Friends and neighbors on the web," *Social Networks*, vol. 25, no. 3, 2003, pp. 211–230.
- [2] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," in *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'06)*, New York, NY, USA: ACM, 2006, pp. 611–617.
- [3] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," in *Proceedings of the National Academy of Sciences*, vol. 99, no. 12, Jun. 2002, pp. 7821–7826.
- [4] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS'01)*. London, UK, Springer-Verlag, 2002, pp. 251–260.
- [5] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th International Conference on World Wide Web (WWW'09)*. New York, USA, ACM, 2009, pp. 551–560.
- [6] N. Shrivastava, A. Majumder, and R. Rastogi, "Mining (social) network graphs to detect random link attacks," in *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering (ICDE'08)*. Washington DC, USA, IEEE Computer Society, 2008, pp. 486–495.
- [7] H.-Y. Lam, and D.-Y. Yeung, "A learning approach to spam detection based on social networks," PhD diss., Hong Kong University of Science and Technology, 2007.
- [8] P. O. Boykin and V. P. Roychowdhury, "Leveraging social networks to fight spam," *Computer*, vol. 38, no. 4, Apr. 2005, pp. 61–68.
- [9] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, "P2p-based collaborative spam detection and filtering," in *Proceedings of the Fourth International Conference on Peer-to-Peer Computing (P2P'04)*. Washington DC, USA, IEEE Computer Society, 2004, pp. 176–183.
- [10] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots + machine learning," in *Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR'10)*. New York, USA, ACM, 2010, pp. 435–442.

- [11] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proceedings of the 10th ACM SIGCOMM conference on Internet Measurement*, New York, USA, ACM, 2010, pp. 35–47.
- [12] M. Fire, G. Katz, and Y. Elovici, "Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies," *Human Journal*, vol. 1, no. 1, 2012, pp. 26–39.
- [13] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in *Proceedings of the ACM SIGCOMM 2010 conference*. New York, USA, ACM, 2010, pp. 363–374.
- [14] M. Abulaish and S. Y. Bhat, "A density-based approach to detect community evolutionary events in online social networks," in *Social Network Analysis and Mining*, R. Alhaji (Ed.), Springer, 2013.
- [15] G. H. John and P. Langley, "Estimating continuous distributions in bayesian classifiers," in *Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence (UAI'95)*, San Francisco, USA, Morgan Kaufmann Publishers Inc., 1995, pp. 338–345.

Biographical Details:

Sajid Y. Bhat is a Ph.D. scholar at the Department of Computer Science, Jamia Millia Islamia, New Delhi-25, India. He is working towards the development of a data mining framework for social network analysis. His research interests span over the areas of Data Mining, Web Intelligence, and Social Media Analysis.

Muhammad Abulaish is currently Associate Professor and Head of the Department of Computer Science, Jamia Millia Islamia, New Delhi-25, India. He obtained his PhD degree from IIT Delhi. He is a senior member of IEEE, ACM, and CSI. His research interests span over the areas of Data Analytics, Social Computing, and Security Informatics. He has published over 65 research papers in journals and conference proceedings. He is a program committee member of several international conferences including CIKM, IEEE/WIC/ACM WI, PAKDD, and KDIR. He also serves as a reviewer for various journals including IEEE TKDE, Digital Investigation, and Information Sciences.