Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Deception Detection in Social Media through Combined Verbal and Non-Verbal Behavior

[1]Dhanyasree P*, [2]Sajitha Krishnan, [3]Ambikadevi Amma T
[1]M.Tech CSE, [2]Assistant Professor, [3]Professor
[1, 2, 3] Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Lakkidi, Kerala, India

Abstract *— **A social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people that have the same interests. Nowadays, social media have a great influence on our daily life. It is really tough to find someone that has not even one account in any of the social media like Facebook, Twitter, Netscape etc. Anyone can create accounts in any social media with less amount of information. Social media give its user a great freedom for having more than one account. This became a serious issue if any misuse use of account is reported. If anyone having more than one account it is termed as socukpuppets. In all existing methods only user's verbal behaviour is considered. An automated system which is able to detect such types of accounts must be necessary for controlling deception through social media. We are proposing a method which use the nonverbal behaviour of the user with less detection time and less time complexity.***

Keywords — social media, Web 2.0, Deception, Sockpuppets, SNM, PSO.

I. INTRODUCTION

Day by day the number of people using social media is increasing. Everything is possible through social media and it became made a drastic change in the way we pursue our social life. Social media has great influence on education, employment, business, etc. Most of the online social networks (OSN) are free. These social media uses web 2.0 technologies. In 1997 the first social media was started but it couldn't survive. Facebook started in 2004 and become world's largest social networking site. Most user benefit is that so many opportunities to connect with their friends and family. The number of people registering in social media like Facebook and Twitter is recorded as 82 % of the total online population. All social media gives more freedom to the user at the same time which leads to identity theft like serious issue[14]. Recently a number of cases were reported and knot about the security issues related to social media. Anyone can create accounts in social media with very less information. The transfer of false information through social media is termed as deception. The explosive growth and influence of social media open the door for new opportunities for deception [3].

Figure 1: Entities on online deception

Figure 1 shows the entities in the online deception process. The deceiver is the one who trying to transfer the false information through social media. Different social media are available. For example it may be Facebook , Twitter, Wikipedia etc. the false information finally transferred to the victim. Social media includes all social networking site, blogs, virtual game worlds, virtual social worlds, content communities and collaborative projects. The necessary to detect such deception through Wikipedia like social media has great impact. If one person having more than one account in Wikipedia, which termed as sockpuppets. Once the sockpuppet cases are found, the admin can either block or ban the user. Block and ban are two different things. If the admin banned a user, he cannot edit some or all Wikipedia pages either temporarily or indefinitely. If the admin blocked a user he cannot edit anymore. Block will be applied to user accounts, IP address for a definite time or indefinite time. Ban is different from blocks because editing is still allowed to rest of the pages. If one user using another person's account which is termed as piggybacking and one using or creating accounts for the purpose of Supporting one side of discussion. Current methods are focusing how to find out the multiple accounts with the verbal behavior of a user. Proposed system trying out to find how we can use the nonverbal behavior of a user. Using Wikipedia as an experimental case, we demonstrate our proposed system.

II. BACKGROUND STUDY

Social media which provide users with a lot of freedom for presenting themselves are in the second row while social media that force users to adapt to certain roles or have no option for disclosing parts of their identities are in the first row. Moreover, with an increase in media richness and social presence, note the transition from social media offering just text

for communication to rich media aimed to simulate the real world using verbal and non-verbal messages as well as more immediacy in communications for virtual game worlds and virtual social worlds[1]. The social networking sites are making our social lives better but nevertheless there are a lot of issues with using these social networking sites. The issues are privacy, online bullying, potential for misuse, trolling, etc [8]. These are done mostly by using fake profiles. In existing system, the verbal behavior of user is used find out the similarity.

Verbal behavior includes name, address, gender, mobile number etc given by the user. Attributes such as name, address, social security number and date of birth from a database were compared as strings using a string comparator and the level of disagreement for these items was obtained between different user records. Furthermore they obtained the overall disagreement between records based on these attributes, and those matches that had a disagreement below a certain threshold were considered as the same account. The most effective solution to identify duplicates in a database with the highest accuracy is a cross-comparison for the full length of accounts in a database. In order to reduce the computational overhead, use adaptation of Sorted Neighbourhood Method (SNM). The original SNM develops a sorting key, sorts a database and then merges the duplicate records using a window of fixed size *w* that moves through the sorted records[13]. The adapted SNM version has a shorter window *w* where *w*' is smaller than *w*. The window in the adapted version is smaller since once a duplicate record is found the rest of the comparisons for a window are ignored. Although these methods yield a high detection accuracy rate, they are computationally inefficient for the social media environment, which often involves databases with large volumes of data.

III. METHODOLOGY

Wikipedia generally includes 28 namespaces. That means 14 subject namespaces and 14 talk namespaces. A namespace is a set of Wikipedia pages. There is article or main namespace, user namespace, file image namespace etc. So in our proposed model, the revisions of different namespaces by user are taken as the nonverbal behaviour of a user. Verbal behaviour includes name, address, gender, mobile number etc given by the user[4].

Attributes such as name, address, social security number and date of birth from a database were compared as strings using a string comparator and the level of disagreement for these items was obtained between different user records. Furthermore they obtained the overall disagreement between records based on these attributes, and those matches that had a disagreement below a certain threshold were considered as the same account. The most effective solution to identify duplicates in a database with the highest accuracy is a cross-comparison for the full length of accounts in a database. Figure 2 shows the user activity and nonverbal behavior. The user revised two times the article page and once he revised the article discussion page. From different revisions we can calculate different nonverbal variables. Current methods are focusing how to find out the multiple accounts with the verbal behaviour of a user. Proposed system trying out to find how we can use the nonverbal behavior of a user. Using Wikipedia as an experimental case, we demonstrate our proposed system.

In our proposed system we are calculating using the nonverbal behavior of the user like each revision. From all that we calculate the different variables. We observe the variations between a legitimate user and sockpuppet. We can plot scatterplot smoothing graph from the observation and understand the changes. We can also compare the results of existing methods and our proposed methods. Sockpuppets must be blocked from the time it is reported. Our proposed system automatically scans each user and findout the sockpuppets [2].

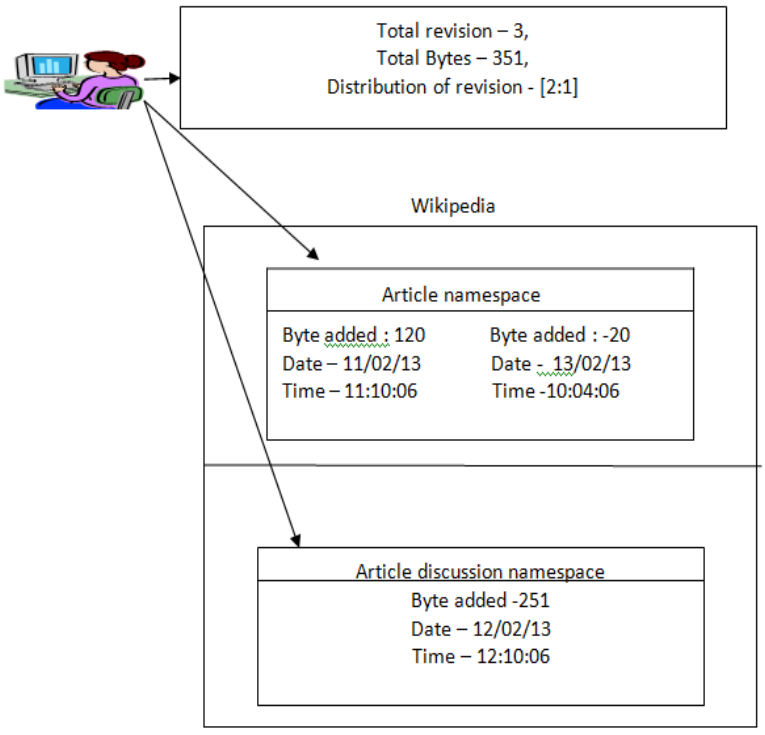

Figure 2: user activity along with nonverbal behaviour

A. Implementation Method To Find Sockpuppets

Multiple accounts create big problems in terms of security and freedom of a user. Motivated by some verbal and nonverbal methods, we propose a modifications to the existing methods and the steps are given below.

1. Calculation of non-verbal variables.
2. Model testing using Random Forest method.
3. Identification of time window using PSO.

B. Nonverbal Calculation

Online variables for a user are categorized into two, time dependent and time independent. The nonverbal variables are number of total revisions (R_t) made by a user for a specific time window since their initial registration with the website. We can easily calculate the number of revisions as they were distributed in the various namespaces such as article(R_{at}). article discussion (R_{dt}), user page (R_{ut}), user discussion page (Rt_t) Wikipedia-related pages and Wikipedia-related discussion pages combined under one variable (RW_t). Other categories added for all the rest of the namespaces such as file uploads images etc (RO_t) . Based on these namespaces, a variable called the Gini coefficient is calculated. Gini coefficient represents differences in activity distribution across these namespaces and is formally defined as,

$$GR_t = 100[\frac{2\sum_{x=1}^{6}(w_x Rx_t \sum_{j=1}^{x} w_j) - \sum_{x=1}^{6} w_x^2 Rx_t}{(\sum_{x=1}^{6} w_x)\sum_{x=1}^{6}(w_x rx_t)} - 1$$

Where *x* represents the revisions on each namespace for this case and the relevant weight denoted by w. The weight w is assigned to each namespace. Equal weights were applied to the data because, conceptually, namespaces on Wikipedia do not hold any weight and any attempt to assign weights would introduce a bias[7]. In addition, it is necessary to calculate the mean number of bytes of bytes added or removed by all revisions:

$$\widehat{\mathrm{RB}}_{\mathrm{t}} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{R_t}} \mathrm{RB_i}}{\mathrm{R_t}}$$

The total number of bytes added (Ba_t) and total number of bytes removed (Br_t) from all the revisions during the observation window were also calculated. Furthermore, the time difference in seconds between the time (TR) a user registered their account until the time of the first revision was measured along with the namespace (FE) where their first revision was made. Finally, the average duration (ADt*)* between revisions was used and is defined as follows:

$$\mathrm{AD_t} = \frac{\sum_{\mathrm{i}=2}^{\mathrm{R_t}} \mathrm{T_i} - \mathrm{T_{i-1}}}{\mathrm{R_t}}$$

It is necessary to calculate a standardized difference between a legitimate user and sockpuppets. For that purpose the difference is represented scatter plot smoothing. For the standardized difference we used the correlation coefficient produced by point-biserial correlation:

$$r_{pb} = \frac{M_1 - M_0}{s_n}\sqrt{\frac{n_1 n_0}{n^2}}$$

C. Time Window Using PSO

We need to set a time window for every user. In the existing methods the time window for newly registered user has a significant impact on effectiveness of the system. For selecting an optimal window, we use the PSO algorithm (Particle Swarm Optimization). PSO optimizes a problem by having a population of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical formulae over the particle's position and velocity. Let *N* be the number of particles in the swarm, each having a position in the search-space and a velocity. In every iteration process, each candidate solution is calculated by the objective function being optimized, which deciding the fitness of that solution [16]. The fitness is computed by

Fitness 1= Min (False Positive rate)

Fitness 2 =Min (Detection time)

Fitness= {Fitness 1, Fitness 2}

The fitness is there is less false positive rate with less time window. The time window values are taken randomly. Then, the existing method is used to detect the malicious users with less time and also with high accuracy. In existing system usually the time window need high detection time. By using proposed method we can reduce the time for detection. , in the proposed method an innovative technique is introduced which is called Selection of Optimum Time window for Identity deception using Non-verbal behavior (OTW-IDNB) for reducing the time complexity. In this method, for selecting the optimal time window the particle swarm optimization algorithm is used. Particle swarm optimization is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. So, based on this algorithm, the optimal time window is used. An experimental result shows that the proposed method achieves less time complexity when compared to the existing system.

IV. RESULT AND DISCUSSION

It is noted that detecting multiple accounts through nonverbal behavior yields more accuracy than existing methods. The automated system to detect multiple accounts gives good performance compared to currently using methods. Both the verbal and nonverbal behavior can be combined and used for sockpuppets detection.

V. CONCLUSION

Social media gives more freedom to its user and the same time it arises some questions about its privacy or security. From all aspects we know that it is easy to create more than one account in all type of social media. The accounts created by a user become a serious issue when it is misused. Throughout this project we are trying to find out how effectively, incorporating with the nonverbal behaviour of a user we can detect the multiple accounts. An automated system will detect more accurately by reducing the time complexity.

As the number of users of internet increases day by day, the number of social media users also increases. Identity theft become common through all social media. This type of thefts increasing and must be blocked for user's security. A social media should provide security to users. Nonverbal behavior gives an alternative path for detecting multiple accounts. Both the verbal and nonverbal behavior can be used for the multiple account detection.

ACKNOWLEDGMENT

First of all we would like to express our gratitude to Almighty . We also thank the department of computer science and engineering for their useful comments and feedback which have helped us to improve the quality and presentation of this paper

REFERENCES

[1] M. Tsikerdekis and S. Zeadally, "Online deception in social media," Commun. ACM, vol. 57, no. 9, Sep. 2014.

[2] T. Solorio, R. Hasan, and M. Mizan, "A case study of sockpuppet detection in wikipedia," in Proc. Workshop Lang.Anal Social Media, pp. 59–68, 2013.

[3] A. C. Squicciarini and C. Griffin, "An informed model of personal information release in social networking sites," in Proc. Int. Conf. Social Comput. (SocialCom) Privacy, Security, Risk Trust (PASSAT), pp. 636–645,2012.

[4] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, "Automatically detecting criminal identity deception: An adaptive detection algorithm," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 36, no. 5,pp. 988–999, Sep. 2006.

[5] M. Neela Malar**,"** Impact of Cyber Crimes on Social Networking Pattern of Girls", International Journal of Internet of Things 2012, 1(1): 9-15

[6] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The Challenges and opportunities of social media," Business Horizons, vol. 53, pp. 59–68, Jan./Feb. 2010

[7] M. Tsikerdekis and S. Zeadally, "Multiple account identity deception detection in social media using nonverbal ", IEEE transactions on information forensics and security, vol. 9 ,no. 8, Aug 2014

[8] P. Ekman and W. V. Friesen, "Nonverbal leakage and clues to deception," Psychiatry: Interpersonal Biol. Process., vol. 32, no. 1, pp. 88–106, Feb. 1969

[9] S. L. Humpherys, K. C. Moffitt, M. B. Burns, J. K. Burgoon, and W. F. Felix, "Identification of fraudulent financial statements using linguistic credibility analysis," Decision Support Syst., vol. 50, no. 3, pp. 585–594, Feb. 2011.

[10] J. S. Donath, "Identity and deception in the virtual community," in Communities in Cyberspace, M. A. Smith and P. Kollock, Eds. London, U.K.: Routledge, 1999.

[12] S. Grazioli and S. L. Jarvenpaa, "Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 30, no. 4, pp. 395–410, Jul. 2000.

[13] J. Hirschberg et al., "Distinguishing deceptive from non-deceptive speech," in Proc. Interspeech, 2005, pp. 1833–1836

[14] X. (Sherman) Shen, "Security and privacy in mobile social network [Editor's Note]," IEEE Netw., vol. 27, no. 5, pp. 2–3, Sep./Oct. 2013.

[15] A. Alfons and M. Templ, "Estimation of social exclusion indicators from complex surveys: The R package laeken," J. Statist. Softw., vol. 54, no. 15, Sep. 2013

[16] Alireza Alfi," Particle Swarm Optimization Algorithm With Dynamic Inertia Weight For Online Parameter Identification Applied To Lorenz Chaotic System", International Journal of Innovative Computing,Volume 8, Number 2, February 2012

,

