Controlling and Mitigating Targeted Socio-Economic Attacks

Prabhat Kumar, Yashwanth Dasari, Shubhangee Nath, Akash Sinha

Controlling and Mitigating Targeted Socio-Economic Attacks

Prabhat Kumar, Yashwanth Dasari, Shubhangee Nath, Akash Sinha

Department of Computer Science and Engineering,
National Institute of Technology Patna, India
{prabhat,dasari134763,shubhangee134784,akash.cse15}@nitp.ac.in

Abstract. The transformation of social media has paved a way to express one's views, ideas, and opinions in an effective and lucid manner which has resulted in its increased popularity. However, there are both pros and cons of this socio-technological revolution. This may lead to its misuse with planned and targeted attacks which often have the potential of massive economic effects. This paper articulates the negative aspects, especially, of how the social media is being misused for greedy needs. Spammers may defame the product to achieve their greedy goal of earning more profit by decreasing the competing effect of their opponents. This paper discusses, analyzes and proposes two novel techniques by which one can either decrease or completely abolish these types of socio-economic attacks.

Keywords: Social Media, Economic, Target Attack, False content prevention, False content tolerance

1 Introduction

Social media has been the ever expanding realm since a decade and has taken the technological advancements to its pinnacle. Social media helps the business in a variety of ways especially in promotion which is economically viable and effective than the traditional ways of promotion. Table 1 enlists the percentage of B2B marketers who use various social media sites to distribute their content. The increasing popularity of social networking sites such as Twitter, Facebook and LinkedIn has attracted a large number of bloggers, content writers and article creators [1]. Social media has removed all the communication and interaction barriers and bridged the gap amongst the earthlings.

Company Name	Percentage(%) of Marketing People using Social Media
Linkedin	91
Twitter	85
Facebook	81
Youtube	73

Google+	55
SlideShare	40
Pinterest	34
Instagram	22
Vimeo	22
Flickr	16
StumbleUpon	15
Foursquare	14
Tumblr	14
Vine	14

Table 1. Percentage of Marketing People using Social Media [2]

Another positive aspect of social media is uniting a large number of people on a huge platform which is necessary to induce positivity in the society. On the other hand, it has many bad and ugly impacts [3]. As stated above our aim is to control or totally mitigate the false content (uploading fake videos which have no authentication, posting vulgar images) making the platform more trust worthy and reliable than the former. Some of the bad and ugly aspects are that some spammers are forging multiple identities (also called Sybil) in order to harm the users of the media [4]. This is due to the fact that no mechanism for authentication is provided when any video or picture that addresses the issue of public interest gets uploaded. One can easily post some false and vulgar content and raise some sensitive issues which may damage the goodwill of the product as it is just a matter of creating a fake identity and uploading a video or some morphed photograph. Cautious content filtration of objectionable or adulterated content is necessary because it is high time to control the evil abuse widely prevalent in the society. This paper provides various approaches to control this at various levels starting from the very root level. The work concentrates on all types of false content detection, false content tolerance and vulgarity issues. The aim is not to undermine the great contributions that the social media has made to social progress and technological advancement but rather to make it more trust worthy, reliable and transform it to a better facilitative tool which supports social cohesion and benign societal relations by abolishing such false content.

2 Related Work

Content-based filtering in online social networks has good results in the case of text or information. Content-based filtering can be applied concurrently at the same time when the text is getting uploaded [10] [11]. But this is not the case with videos or photographs. Daily millions of videos get uploaded and content filtration is not possible. Even the technique of content-based filtration is context based. Much of the literature work is not available in this context of socio-economic attacks. Some of the available instances are Maggi incident and many messages spreading that soft-drinks

are contaminated with AIDS blood etc. Such incidences clearly elucidate some of the ugly aspects of social media.

Ying-Chiang-Cho addressed various negative aspects of social media such as 1) Cyber Bullying, 2) Role of social media in organization of negative social events such as the 2011 UK riots, 3) Social-media-assisted infidelity and promiscuity [3]. He has discussed various instances of the misuse of social media in different public domains. One of them is Cyber bullying which describes the situation of a child or a teenager when he/she is harassed, humiliated, embarrassed, threatened or tormented using the digital technology. Cyber bullying includes sending mean messages or threats, spreading rumors, posting hurtful or threatening posts, sexting (circulating sexually suggestive pictures or messages about a person) and so forth [5] [6]. He articulated the ugly side of social media by various examples. Some of them are as follows:

- A 13-year old school boy, Ryan Halligan took his life because of cyber bullying.
- A 15-year old girl, Phoebe Prince hanged herself because of the threatening messages and called names at school.

There are still many instances which have not come under the limelight in the society. His work has addressed the issues very well but has provided no means of abating or eradicating the serious threat from the society. His work also lacks the discussion of any socio economic attacks [3]. R.Gandhi et al. has addressed the economic issues related to security [8]. His work has paved ways for the future extension of such critical issues in the context of economy such as damaging the reputation of perishable goods. This work includes providing solution to this critical issue at various stages. The work includes abating it at the very rudimentary level, tolerating it at the middle and the peak stages. Posting of fake videos and photographs may damage the goodwill of the good to a major extent. We are paying special attention to this type offensive videos and photographs which publicize the objectionable and fake content which has no source of authentication in it-self.

3 Strategies

We propose two techniques namely 1. FALSE CONTENT TOLERANCE and 2. FALSE CONTENT PREVENTION. To illustrate these techniques let us consider the following scenario. Say, a plate contains five types of fruits namely apples, oranges, mangoes, bananas and grapes that constitute the daily supplements of an individual in the country, India. The usual cost of apples and grapes is higher than the others. So we can categorize these as costly fruits. The cost of mangoes and oranges is greater than that of bananas but cheaper than apples and grapes. So these can be categorized as medium cost fruits. The cost of bananas is far cheaper than the others. So this fruit can be categorized as a low cost fruit.

The country India exhibits a large proportion of population of average and low salaried people. This infers that an average salaried person generally resorts to buying or ordering either medium cost fruits or low cost fruits. So the demand for medium and low cost fruits is higher, again amongst these, the demand for low cost fruit

dominates. Without loss of generality the restaurant managing personnel will have a greater quantity of bananas, a medium quantity of mangoes and oranges, and a lower quantity of apples and grapes. Suppose the managing staff of mango production unit wishes to raise the demand for mangoes in the market so as to increase the net profit of the production unit. To achieve this, the unit plans a scheme to decline the popularity of other fruits in the market. The competitors in this scenario are apples, grapes, oranges and bananas. As the cost of apples and grapes are higher, the competing effect of these fruits can be neglected. So the real competitors are oranges and bananas in which the competing effect of bananas is higher than that of oranges. Hence they would like to target the sales of bananas and oranges. The plot is as follows: The production unit will create a video which tarnishes the popularity of the target fruits, oranges and bananas. In the video, they may use all types of defaming contents which shows that eating these fruits will spoil the health of common mass and will show side effects in the upcoming future. Also the video may make some false claim that this video is approved by some of the well known, reputed doctors or health societies. Further as the present social media does not provide any authentication for posting of these types of videos, this video may go viral in the social media negotiating the genuineness of the target fruits, oranges and bananas achieving the goal of the production unit successfully. In due course of time, the video gets popularized in all the sections of the society. This may not have any drastic effect on consumption of that particular fruit if an individual is considered. But as a whole this may have a serious decline in consumption of the target fruits and therefore also reducing the profits. This may have a drastic impact on the sales of these target fruits. Everyone may start to pick a mango instead of taking an orange or a banana. Gradually the demand for mangoes will sharply increase and the market price of mango will soar. Thereby the target of mango production units is achieved easily just by posting a fake video which has no authentication at all. The same thing can be done by many adversaries for spoiling the goodwill of their opponents in one or the other way. This is a serious issue which needs urgent consideration.

To cater the need of addressing such issues we propose techniques to reduce or possibly diminish the effect of this false content. The FALSE CONTENT TOLERANCE approach aims at minimizing the fake post by associating the information of the user with the post he uploads. In this strategy, the social media allows all types of videos to get posted. Possibly the video may be seen by an individual and he/she starts sharing it. If a video is getting shared, it should be shared along with the source id's URL (who posted it for the first time) should also be shared. If this type of control mechanism is implemented these false content videos may reduce to an appreciable amount as the source identity can be known easily from the URL. So the spammers may have the fear of their identity getting easily traced. For example, instances of false content promotions or defamation of rival products administered through uploading and sharing of videos and other media are witnessed on the social networking sites like Facebook, Twitter etc. on a routine basis. Now if it is made mandatory to reveal one's source id and that the aforementioned detail is displayed publicly along with the given video or other media then the culprit might get apprehensive about being publicly shamed or subjected to persecution through law. He

knows that now he can be traced till a certain point. So, it is safe to conclude that a general disinclination towards uploading of such false videos and other media may be evident post implementation of the aforementioned technique. This requires very few changes in the existing framework and the present architecture of the social media. As it requires very few changes, it only requires a minimum effort to do this work. But still the users can make Sybil accounts (fake id) and do this type of unethical things to fulfill their greedy need of tarnishing a product. Hence the problem still persists which can be resolved by using FALSE CONTENT PREVENTION technique.

The second technique is illustrated as below: When a video is posted the social media authorities ask for the user's telephone number as an authentication mechanism. The OTP mechanism can be used to verify the user's telephone number. If this type of authentication is done successfully then those videos are called certified videos. The user's telephone number will not be shared and will be kept safe and secure by the social media authorities. If the user refuses to reveal his identity the social media still allows to post the video but these videos are called uncertified videos. Such videos can still be shared but they lose their credibility. This ensures that the video having fake content may not get popularized. The additional changes in the settings of giving the option to show only certified videos help to reduce the effect in a very effective manner. This requires more effort than the tolerance technique but ensures that the fake content is not encouraged in any manner.

4 Analysis

The tolerance strategy though requires minimal changes in the existing architecture and the present framework is not at all a viable solution because it is just a matter of few minutes to create one fake id. These types of fake ids persist in all types of social networks. Albeit the prevention strategy requires much effort and time but it guarantees the addressing of the problem from the very root level. The effort involves changing the settings architecture, an overhead of time and effort during authentication and also verifying whether the video is certified or not during the time of sharing. This technique has an authentication mechanism by which the user can be tracked easily by the means of telephone number which is re-verified using OTP (One Time Password). So the user cannot simply escape by giving a false telephone number. As the certified videos can only be shared by using this technique, it has an indirect effect of gradually diminishing this sort of misuse in all contexts. If an annotation of 'recommended for most of the users' is provided along with the option of show only certified videos, then most of the users will go for it. Gradually it gets popularized and spreads from one user to another resembling the chain effect. Consequently, only the certified videos get posted and also only those videos are shared.

Just like prevention is better than cure, the prevention strategy stated above is better than the tolerance strategy.

5 Conclusion

Careful and selective content filtration is essential so as to stop socio economic back-stabbing which may have a serious business effect [7] and [8]. Our proposed methods work well in all platforms. The technique of false content prevention is much viable and reliable than the false content tolerance though it requires more effort. Validation of fake videos (if reported by an organization or a company to social media authorities) and posting new videos along with certification to counter the false attacks (counter videos) addresses the problem in an effective way. Further this can also be applied to contents such as textual posts which are abusive and non-ethical. However, the proposed techniques suffer with certain limitations as in case of FALSE CONTENT TOLERANCE which can be defeated by using Sybil accounts. The prevention approach provides an improvement over the tolerance strategy but requires a certain overhead from implementation point of view. These techniques can be improved in the future by real time implementation and proper feedback integration. In addition, the rating of videos based on its authenticity may help to make the platform more trustworthy.

References

1. Spisak, K., Social Media Statistics (2015).: http://www.business2community.com/social-media/social-media-statistics-2015-01393793#IPjuq80WDr2XirGf.97
2. Pulizzi, J., B2B Content Marketing: 2014 Benchmarks, Budgets, and Trends—North America (2014).: http://contentmarketinginstitute.com/wp-content/uploads/2013/10/B2B_Research_2014_CMI.pdf
3. Cho, Y. C.: Violence and Aberration in the Age of Social Media: Transforming the advanced communication technology into a better facilitative tool, IEEE Consumer Electronics Magazine, 3(4), 69-74 (2014)
4. Koll, D., Li, J., Stein, J., Fu, X.: On the state of OSN-based Sybil defenses, In: Networking Conference, 2014 IFIP, 1-9. Trondheim, (2014)
5. Bullying Statistics.: http://www.bullyingstatistics.org/content/cyber-bullying-statistics.html.
6. Cyberbullying Case Studies.: http://cyberbullying.ua.edu/index.php/casestudies/
7. Oehri, C., Teufel, S.: Social media security culture, In: Information Security for South Africa, ISSA 2012, 1-5. Johannesburg, Gauteng (2012)
8. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, IEEE Technology and Society Magazine, 30(1), 28-38 (2011)
9. Saaty, T.L., Ozdemir, M.S.: Why the magic number seven plus or minus two, Mathematical and Computer Modelling, 38(3–4), 233-244 (2003)
10. Thilagavathi, N., Taarika, R.: Content based filtering in online social network using inference algorithm, In: International Conference on Circuit, Power and Computing Technologies, ICCPCT 2014, 1416-1420. Nagercoil (2014)
11. Vanetti, M., Binaghi, E., Carminati, B., Carullo, M., Ferrari, E.: Content-based filtering in on-line social networks, In: Priv Secur Issues Data Min Mach Learn., 6549, 127–40. Springer, Berlin, Heidelberg (2011)