Preventing Deception from Online Social Media using Deception Matrix

Alka[1], Harjot Kaur[2]

[1]*Department of Computer Science, GNDU Regional Campus Gurdaspur, Punjab, India*
[2] *Department of Computer Science, GNDU Regional Campus Gurdaspur, Punjab, India*

ABSTRACT- *The organization collaboration is very important for the success of the organization. The persons who enter into the organization will interact with the other members of the organization. There exist leaders of the community who are responsible for the management of the communication among the persons within the organization. Sometimes the information presented by the new person joining the community is not correct. This information will cause the deception over the network. In the proposed paper, deception within the social media is going to be analyzed by using the concept of deception matrix. Deception will cause legion of problems and sometimes death of the person who is deceived. The proposed paper suggests the mechanism for tackling such deceptions.*

Keywords- Collaboration, interact, information, deception, social media

1. INTRODUCTION

The proliferation of web based technologies have modified the way that the content is generated and exchanged through the Internet, leading to proliferation of social media applications and services. Social media like Facebook enable creation and exchange of user generated content and design of range of Internet based applications. The services provided by the Internet have increased. This not only provides the extra facilities to the users but also has attracted large number of users towards the Internet based technologies. As more and more users are intended toward the Internet so does the social networking sites. In today‟s environment there exists a large number of social networking websites. These social networking websites use large number of interactive mechanisms to impress the users. Each social networking website needs user. So these social networking sites do not use any solid foolproof mechanism of authentications. This can cause frauds over the social networking sites.

From previous work on deception, it has been found that people in general lie routinely and several efforts have been made to detect and understand the deception. Deceptions have been used in various contexts throughout human history to enhance attacker‟s tactics. Social media provides new environments and technologies for potential deceivers. There are many examples of people being deceived through social media, with some suffering from devastating consequences in their personal lives. Deception in the proposed system will be considered the deliberate attempt to mislead others. In deception the person who is deceived may not be aware of the fact that he/she is becoming deceived. The deception will be more profound in the area where boundary between privacy and deceiving others is not clear. The proposed system will be used in order to introduce the security mechanism known as *physical check mechanism* to ensure that the account on the social networking websites can only be created if the background check is successfully performed.

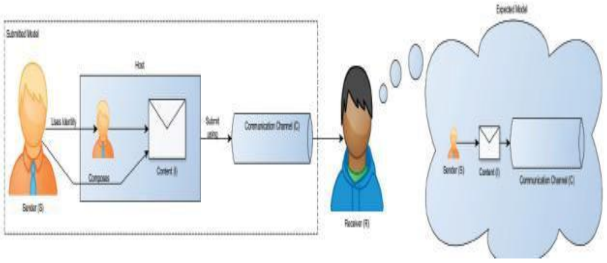


Fig 1. Role of deception in interaction

METHODS

Participants and procedure

A message inviting people to answer a web-based questionnaire was posted in 14 discussion groups. These discussion groups were randomly selected from three different popular Israeli portals. These discussion groups varied in content, and included both groups that discuss a particular subject (e.g., meteorology, internet culture, or new age) and groups that have more general, unspecific topics (like a group for 30+, university students, or males).

A total of 257 people returned the questionnaire; 68% reported being female. The reported mean age was 30 (range: 14–70), with the following distribution: 17% under the age of 20, 44% 20–30, 27% 30–40, and the rest over
40. Seventy-nine percent reported having an academic education (students in higher education institutes or postgraduate). On the average, people reported spending
3.5 h per day online (range 0.5–18 h). Average reported on- line competence was 3.2 points (out of

5); 64% re- ported higher than 3.5 points in this measure.

Instrument

A two-part "Deception Questionnaire" was constructed. The first part included the following questions asked on five-point Likert scales (where 1 = not prevalent/never, and 5 = highly prevalental ways: (1) In your opinion, to what extent is online deception (someone who intentionally gives incorrect details about himself) prevalent? (2) Have you ever deceived online? (3) Have you ever sensed that someone has deceived you online? Those who ad-mitted to having deceived online at least once were asked to mark all issues about which they gave incorrect information when deceiving someone online. The issues were age, sex, residence, marital status, height, weight, sexual preference, health status, occupation, a salient personality trait, or something else (if the last option was marked, respondents were asked to provide details). For each of the issues marked, respondents were asked to mark what motivated them most to do so. The options were (a) safety reasons, (b) identity play, (c) changing status, and (d) increased attractiveness. Next, they were asked if they felt that others suspected it was false information. In addition, they were asked to mark the emotions that they experienced while deceiving online. Emotions included tension, excitement, enjoyment, stress, oddness, and "another feeling."

The second part of the questionnaire asked for demographic details (age, gender, hours online and occupation) and online competence. Online competence was an average score of nine items that the respondents were asked to report their competence with (where "1" means have no competence and "5" means being highly competent). The nine competence items were: searching for information over the Internet, participating in asynchronous discussion groups, participating in chat rooms, downloading music and movies, using e-mail, using online banking, buying online, participating in online games, and using online dating services. Since this is a first attempt to explore online deception among Israeli users, no external references or criteria were available to test the external valid-ity of the questionnaire. Since participants acted anonymously, reliability (pretest/posttest stability) could not be tested. However, as will be discussed later, the results are similar to those reported for other populations.

2. RELATED WORK

Deception will cause legion of problems. Some problems are significant and some are just for matter of laugh. The work has been done toward the deception within the social media presented by Hancook [1] The concept of digital deception is presented in this case. The mechanism of deception is caused because human being nature is to lie. There are efforts which are made in order to detect the deception within the social media. But no solid mechanism is suggested. So analysis of all the techniques which are present will be performed in this paper. In the past decade, [2] social networking services (SNS) flooded the Web. The nature of such sites makes identities deception easily, offering a quick way to set up and manage identities, and then connect with and deceive others. Fighting deception requires a coordinated approach by users and developers to ensure detection and prevention. This article identifies the most prevalent approaches in detecting and preventing identity deception (from both a user's and developer's perspective), evaluating their efficiency, and providing recommendations to help eradicate this issue. As presented by Tsikerdekis and Zeadally [3], Internet is becoming more exposed to the users, so does its vulnerabilities. There exists wide variety of users over the internet. The intentions of all the users will not be certain. So, the person with the wrong intentions may cause the problem over the online social media. This deception is analyzed within this paper. Vishwa nath (2014) have discussed that: What makes deceptive attacks on social media particularly virulent is the likelihood of a contagion effect, where a perpetrator takes advantage of the connections among people to deceive them. To examine this, the current study experimentally stimulates a phishing type attack, termed as farcing, on Facebook users. Farcing attacks occur in two stages: a first stage where phishers use a phony profile to friend victims, and a second stage, where phishers solicit personal information directly from victims. In the present study, close to one in five respondents fell victim to the first stage attack and one in ten fell victim to the second stage attack. Individuals fell victim to a level 1 attack because they relied primarily on the number of friends or the picture of the requester as a heuristic cue and made snap judgments.

Victims also demonstrated a herd mentality, gravitating to a phisher whose page showed more connections. Such profiles caused an upward information cascade, where each victim attracted many more victims through a social contagion effect. Individuals receiving a level 2 information request on Facebook peripherally focused on the source of the request by using the sender‟s picture in the message as a credibility cue. Chen and Huans (2011) in [5] discuss that the increased use of emerging digital platforms as new tools in communication has become an integral part of business activities and the social lives of many individuals. Given the Internet‟s vulnerable design, however, the rapid growth of online deception poses an extremely serious problem, and there is still little scholarly work on this issue. Using online deception cases from Taiwan, the authors undertook the current study with a twofold objective: (1) to investigate the distribution and patterns of deception tactics, and (2) to test hypotheses about how the identity of a potential victim and the purported identity of the deceiver affect the selection of a specific deception tactic.

They found that the selection of deception tactics is significantly influenced by the characteristics of the deceivers and their targets. Implications of their results are also discussed. Keywords: Electronic commerce, online deception, deception tactics, content analysis, logistic regression In [6], Tsikerdekis and Zeadally (2015). The unknown and the invisible exploit the unwary and the uninformed for illicit financial gain and reputation damage.

From the above it has been analyzed that the previous work does not concentrate in ensuring a strong background check mechanism in order to ensure that user with mollified intention shall not able to create account over the social media. The proposed model will suggest a strong background check mechanism to ensure that the deception over the social media can be reduced.

3. PROPOSED MODEL

The proposed model is going to create a system in which the information presented by the user will be passed through the filter. That filter will verify the information presented by the user. In case, the information presented by the user is false then legal action can be taken against him/her. The proposed model will ensure that the deception over the network can be reduced. This paper introduces the concept of jail also. If the person lies, then its account will be sealed. The person will be punished in the case of deception. The deception matrix is created in order to verify whether person is deceptive or not. The set of parameters are included within the deception matrix. If all the parameters are successfully satisfied then the person is not deceptive. The structure of the deception matrix is as follows:

Phone No	E-Mail	School	College	Deception
1	1	1	1	False
1	0	1	1	True
1	1	0	0	True
0	0	0	0	True
1	1	1	1	False

Table 1: Contents of the Deception Matrix

The presence of 1s in cells of the deception matrix indicate that corresponding condition is satisfied and the presence of 0‟s in the deception matrix indicate that corresponding condition is not satisfied. The failure of even single parameter will result in the deceptive agent declaration. This matrix will be critical in determination of fair and deceptive agents. For performing the background check of various users, a background check algorithm will be functioning, which will decide whether the user is deceptive or not.

The *background check algorithm* can be stated as follows:

```
Algorithm Backgroundcheck()

// This algorithm builds a network and receives
information ($I_n$) from the user (U) and then
performs validation mechanism to verify

the data present in it.

1) Record Length of the Record (Rf) in $I_n$.

2) Loop until I > 0
    a) Make user (U) pass through the
       series of Questions (Q).
    b) If InValid(Q) then
  B1) Declare user as False (F) and return
```

```
            Else
    B2) Goto c End if

        c)  Perform BackgroundCheck(B)

        d)  If IsValid(B) then
    D1) Declare user (U) as Valid and goto step e.
            Else
    D2) Declare user (U) as InValid.
            End if

        e)  I=I-1
                End
                Loop
        3)  Stop
```

The above algorithm suggests that the user has to go through series of steps before user will be able to create account over the network or social media. The questionnaires are also used so that validity of the user can be verified.

3. RESULTS

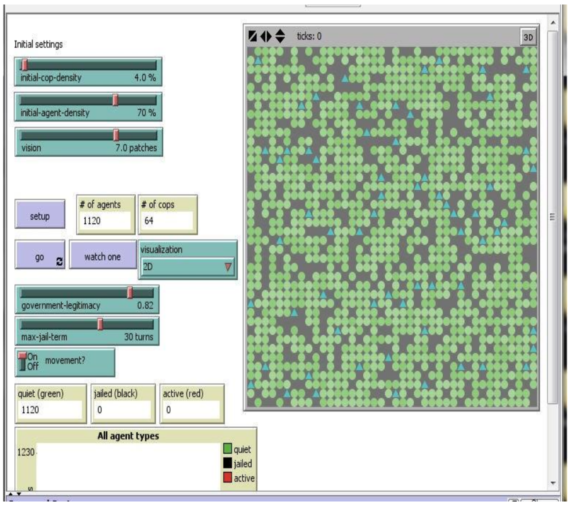
The following table shows age-wise deception which occurs over the social network like facebook.

AGE AND INTERNET COMPETENCY DIFFERENCES IN DIFFERENT ISSUES OF DECEPTION

		Internet Competency	
Factors	*Age differences*	*Differences*	*Frequency of use*
Sex	No difference	No difference	Frequent > Infrequent, $y^2(1) = 17.69$, $p < 0.001$
Age	Younger > Older $y^2(3) = 9.75$, $p < 0.05$	Competent > Non-Competent $y^2(1) = 7.27$, $p < 0.01$	Frequent > Infrequent, $y^2(1) = 8.36$, $p < 0.005$
Residency	Younger > Older $y^2(3) = 10.73$, $p < 0.05$	Competent > Non-Competent $y^2(1) = 7.27$, $p < 0.01$	Frequent > Infrequent, $y^2(1) = 4.46$, $p < 0.05$
Marital status	No difference	Competent > Non-competent $y^2(1) = 8.18$, $p < 0.005$	Frequent > Infrequent, $y^2(1) = 4.45$, $p < 0.05$
Occupation	No difference	No difference	Frequent > Infrequent, $y^2(1) = 6.98$, $p < 0.01$

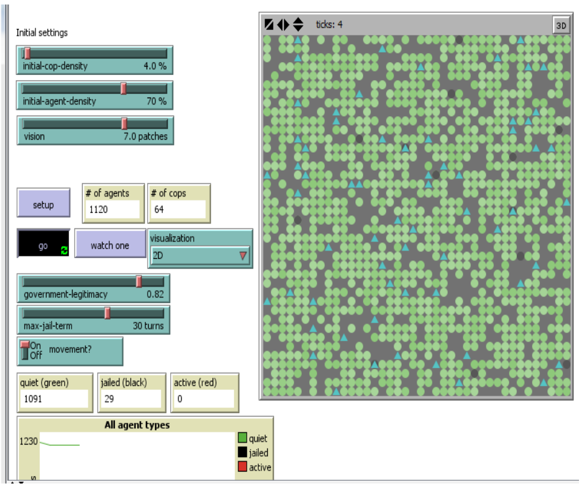
Table 2. Age-wise description of deception in users

The above described agent-based deception model for performing background check mechanism is created in NetLogo. The deception will be handled by the use of leader of the community. The new user will enter into the system and interact with the leader. If leader allows the new agent to enter into the system then its credentials will be checked. If the credentials are not valid, then the new agent entering into the system will be jailed. The concept of jailed will be used to handle the deception present within the online social media. The screen shots of the proposed system will be as follows.



Initial settings
initial-cop-density 4.0 %
initial-agent-density 70 %
vision 7.0 patches
# of agents 1120
# of cops 64
visualization 2D
government-legitimacy 0.82
max-jail-term 30 turns
movement? On
quiet (green) 1120
jailed (black) 0
active (red) 0

Fig 2. Agent-based model created in NetLogo


Initial settings

initial-cop-density 4.0 %

initial-agent-density 70 %

vision 7.0 patches

# of agents 1120

# of cops 64

visualization 2D

government-legitimacy 0.82

max-jail-term 30 turns

movement? On

quiet (green) 1091

jailed (black) 29

active (red) 0

ticks: 4

Fig 3. Background Check mechanism being performed in NetLogo

The diagnosed agent types in the model are plotted in the graph as follows:

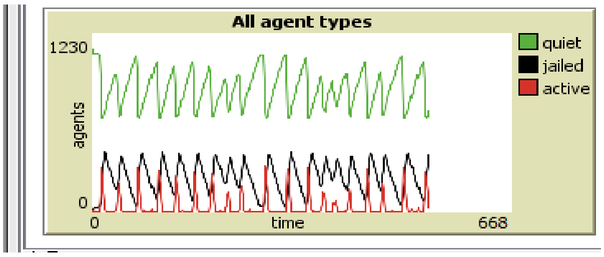


Fig 4 Diagnosed agent types in the model

5. CONCLUSIONS AND FUTURE WORK

The deception can be the big problem which is present within the social media. Detecting the deception and imposing the fine on them is the prime objective of this paper. This paper proposes the background check mechanism in order to ensure that deception never occurs in the system. The technique suggested in this paper, efficiently detects and resolves the problems present within the online social media like Facebook. The main problem that is present within the proposed technique is that it is very time consuming to perform such a background check. So, in future we will try to invent a new technique in order to resolve the issue of time consumed in background check mechanism.

REFERENCES

[1] S. Bandyopadhyay and R. Bhattacharya, "On some aspects of nature-based algorithms to solve multi- objective problems," *Stud. Comput. Intell.*, vol. 427, pp. 477–524, 2013.

[2] J. T. Hancock, "Digital Deception: Why, When and How People Lie Online," *Oxford Handb. Internet Psychol.*, pp. 289–301, 2007.

[3] M. Tsikerdekis and S. Zeadally, "Detecting and Preventing Online Identity Deception in Social Networking Services," *IEEE Internet Comput.*, vol. 19, no. 3, pp. 41–49, May 2015.

[4] "The Stranger Among Us: Identity Deception in Online Communities of Choice | Patricia J Moore - Academia.edu." [Online]. Available: http://www.academia.edu/1629343/The_Stranger_Among_Us_Identity_Deception_in_Online_Communit ies_of_Choice. [Accessed: 25-Feb-2016].

[5] A. Vishwanath, "Diffusion of deception in social media: Social contagion effects and its antecedents," *Inf. Syst. Front.*, vol. 17, no. 6, pp. 1353–1367, Jun. 2014.

[6] C.-D. Chen and L.-T. Huang, "Online Deception Investigation: Content Analysis and Cross-Cultural Comparison," *Int. J. Bus. Inf.*, vol. 6, no. 1, pp. 91– 111, 2011.

[7] T. U. Delft and R. Magnificus, *Agent-Based Modeling of Culture ' s Consequences for Trade Proefschrift*. 2011.

[8] J. Yuill, J. Yuill, D. Denning, D. Denning, F. Feer, and F. Feer, "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques," *Techniques*, vol. Journal of, pp. 26 – 40, 2006.

[9] "Online Deception in Social Media." [Online]. Available: http://cacm.acm.org/magazines/2014/9/17 7936- online-deception-in-social-media/abstract. [Accessed: 09-Feb-2016].

[10] J. Lehman and R. Miikkulainen, "Overcoming deception in evolution of cognitive behaviors," in *Proceedings of the 2014 conference on Genetic and evolutionary computation - GECCO '14*, 2014, pp. 185–192.

[11] J. Wolak, D. Finkelhor, K. J. Mitchell, and M. L. Ybarra, "Online „predators‟ and their victims: Myths, realities, and implications for prevention and treatment.," *Am. Psychol.*, vol. 63, no. 2, pp. 111–128, 2008.

[12] D. P. Twitchell, J. F. Nunamaker, and J. K. Burgoon, "Using speech act profiling for deception detection," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3073, 2004.