

# Detection of Manipulated Communications in a Q&A Site

## by Considering Time Lags between Answer Submission and Problem Resolution

Yasuhiko Watanabe, Kenji Umemoto, Ryo Nishimura, and Yoshihiro Okada

Ryukoku University

Seta, Otsu, Shiga, Japan

Email: watanabe@rins.ryukoku.ac.jp, t070400@mail.ryukoku.ac.jp,

r\_nishimura@afc.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

**Abstract**—Some users of Question and Answer (Q&A) sites use multiple user accounts and attempt to manipulate communications in the site. Manipulated communications, especially, manipulated evaluations, decrease the credibility of the Q&A site. In order to detect manipulated communications in a Q&A site, in this paper, we propose a method of detecting users suspected of using multiple user accounts and manipulating communications in a Q&A site by considering time lags between answer submission and problem resolution. We show our method is useful for detecting inadequate multiple account users and their submissions. In this study, we used the data of Yahoo! chiebukuro, one of the most popular Q&A sites in Japan, for observation and examination.

**Keywords**—*manipulated communication; multiple account user; Q&A site; time lag; credibility.*

### I. INTRODUCTION

These days, many people use Question and Answer (Q&A) sites. They share their information and knowledge by submitting questions and answers in Q&A sites. Q&A sites offer greater opportunities to users than search engines because of the following:

- Users can submit questions in natural and expressive sentences, not keywords.
- Users can submit ambiguous questions and still receive some answers from other users.
- Communications in Q&A sites are interactive. Users have chances to not only submit questions but give answers and, especially, join discussions.

Furthermore, Q&A sites are more convenient than Social Network Service (SNS) sites because of the following:

- Information in Q&A sites is reliable. This is because information in Q&A sites is generally checked and evaluated by questioners. Questioners in Q&A sites usually show which answers are useful to solve their problems.
- It is easy to retrieve communication records and find information for problem resolution. This is because information in Q&A sites is recorded in the form of questions and their answers.

As a result, Q&A sites are a promising media. Two of the essential factors in Q&A sites are anonymous submission and evaluation. In most Q&A sites, user registrations are required for those who want to join the Q&A sites. However, registered users generally need not reveal their real names to submit messages (questions, problems, answers, opinions,

etc.). It is important to submit messages anonymously to a Q&A site. This is because anonymity gives users chances to submit messages without the potential privacy risks of disclosing personal information. However, some users abuse the anonymity and attempt to manipulate communications in a Q&A site. For example, some users use multiple user accounts and submit messages to a Q&A site inadequately. Manipulated communications (especially, manipulated evaluations) discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. As a result, it is important to detect users suspected of using multiple user accounts and manipulating communications in a Q&A site. Previous user identification methods can be categorized into two kinds of approaches.

- identity tracing based on user accounts and
- authorship identification based on analyzing stylistic features of messages.

In this case, identity tracing based on user accounts is not effective because inadequate users often attempt to hide their true identity to avoid detection. A possible solution is authorship identification based on analyzing stylistic features of messages. In recent years, a large number of studies have been made on authorship identification. However, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in a Q&A site. To solve this problem, Watanabe et al. proposed a method of detecting users suspected of using multiple user accounts and manipulating evaluations in a Q&A site [1]. This method was based on one idea: inadequate multiple account users give too many good evaluations to their submissions. In other words, this method can be classified into authorship identification based on analyzing users' behaviors in anonymous communication services. This inadequate submission detection was useful but not enough because there are several types of inadequate submissions. To detect inadequate submissions more widely, in this paper, we propose a new method of detecting inadequate submissions by considering time lags between answer submission and problem resolution. We used messages in the data of Yahoo! chiebukuro [2], a widely-used Japanese Q&A site, for observation and examination.

The rest of this paper is organized as follows: In Section II, we survey the related works. In Section III, we describe multiple account users in a Q&A site. We explain Yahoo! chiebukuro which we take for an example of Q&A sites. In Section IV, we propose a method of detecting unnatural submissions in a Q&A site by considering time lags between answer submission and problem resolution. In Section V, we

TABLE I. THE NUMBERS OF USERS AND THEIR MESSAGES SUBMITTED TO PC, HEALTHCARE, SOCIAL ISSUES CATEGORY AND ALL 286 CATEGORIES IN YAHOO! CHIEBUKURO (FROM APRIL/2004 TO OCTOBER/2005).

category	$U_{qst}$	$N_{qst}$	$U_{ans}$	$N_{ans}$
PC	43493	171848	27420	474687
healthcare	29954	84364	38223	289578
social issues	13259	78777	25766	403306
all 286 categories	165064	3116009	183242	13477785

(Note)  $U_{qst}$  and  $U_{ans}$  are the numbers of users who submitted questions and answers, respectively.  $N_{qst}$  and  $N_{ans}$  are the numbers of questions and answers, respectively.

apply our method into a Q&A site and show that the method is useful for detecting inadequate submissions in a Q&A site. Finally, in Section VI, we present our conclusions.

## II. RELATED WORKS

One of the essential factors of the Internet is anonymity. However, Internet users are generally concerned about unwanted audiences obtaining personal information. Joinson discussed the anonymity on the Internet from various points of view [3]. Fox et al. reported that 86% of Internet users are concerned that unwanted audiences will obtain information about them or their families [4]. Kambourakis pointed that anonymity is necessary in almost any protocol, application or service used in wired or wireless networks, and showed a survey on anonymity preserving solutions [5]. However, these days, many users abuse the anonymity. Take a Sybil attack for example. In a Sybil attack, the attacker intends to gain large influence on a peer-to-peer (P2P) network by creating and using a large number of pseudonymous identities [6] [7]. Sybil attack is a cheap and efficient way to gain large influence on P2P networks [8]. Similarly, in human online communities, such as, web-based bulletin boards, chat rooms, and blog comment forms, many users are thought to use multiple user accounts inadequately and submit inadequate messages, such as deceptive opinion spams. In recent years, a large number of studies have been made on authorship identification [9]–[14]. However, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in the Internet. One of the difficulties of this problem is that we did not have sufficient number of examples of inadequate multiple account users and their submissions. To solve this problem, some researchers tried to extract inadequate submissions by using heuristic methods based on text similarities and ranking results [15] [16]. On the other hand, the authors of [17] pointed that these heuristic methods were insufficient to detect inadequate submissions precisely, and showed they could detect inadequate submissions precisely when they used large number of examples of inadequate submissions. However, they obtained examples of inadequate submissions by using Amazon Mechanical Turk [18]. The examples of inadequate submissions created by workers in Amazon Mechanical Turk have the following problems.

- Little is known about the purposes and methods of inadequate submissions. As a result, it is possible that their instructions to workers in Amazon Mechanical Turk were insufficient.

- There are unreliable workers in Amazon Mechanical Turk [19].

As a result, it is important to obtain inadequate submissions from the Internet. To solve this problem, we proposed methods of detecting inadequate multiple account users and their submissions [1]. This method can be classified into authorship identification based on analyzing users' behaviors in anonymous communication services. However, as mentioned, little is known about the purposes and methods of inadequate multiple account users. As a result, it is important to investigate these inadequate multiple account users and their inadequate submissions from various points of view.

## III. MULTIPLE ACCOUNT USERS IN A Q&A SITE

In this section, we take Yahoo! chiebukuro for example and discuss reasons why and how some users in a Q&A site use multiple user accounts.

### A. Yahoo! chiebukuro

Yahoo! chiebukuro is a Japanese version of Yahoo! answers and one of the most popular Q&A sites in Japan. In Japanese, chiebukuro means "bag of wisdom". Users of Yahoo! chiebukuro submit their questions and answers in the next way.

- User registrations are required for those who want to join Yahoo! chiebukuro.
- Users need not reveal their real names to submit their questions and answers.
- Each user can submit his/her answer only one time to one question.
- The period limit for accepting answers is one week. However, questioners can stop accepting answers before the time limits.
- After the time limits, questions with no answers are removed and cannot be referable. On the other hand, questions with answers can be referable.
- Each questioner is requested to determine which answer to his/her question is best and give a *best answer* label to it.

In this study, we used messages in the data of Yahoo! chiebukuro for observation and examination. The data of Yahoo! chiebukuro was published by Yahoo! JAPAN via National Institute of Informatics in 2007 [2]. This data consists of about 3.11 million questions and 13.47 million answers which were posted on Yahoo! chiebukuro from April/2004 to October/2005. In the data, each question has at least one answer

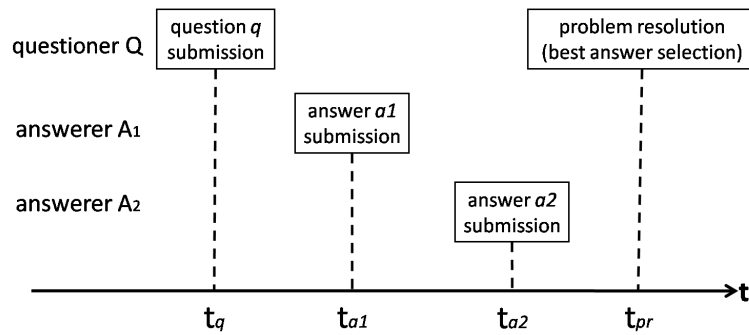


Figure 1. An example of a series of events that occur after a questioner submits his/her question to a Q&A site. Questioner  $Q$  submitted question  $q$  at  $t_q$ . Also, answerer  $A_1$  and  $A_2$  submitted their answers at  $t_{a1}$  and  $t_{a2}$ , respectively. Finally, questioner  $Q$  stopped accepting answers and determined which answer was the best answer at  $t_{pr}$ .

TABLE II. THE CUMULATIVE RELATIVE FREQUENCY OF TIME LAGS BETWEEN SUBMISSION TIME OF ANSWER  $T_A$  AND PROBLEM RESOLUTION TIME  $T_{PR}$  IN THE DATA OF YAHOO! CHIEBUKURO.

cumulative relative frequency (%)	0.5	1.0	1.5	2.0	2.5	5.0	...	50.0
time lag between $T_a$ and $T_{pr}$ (sec)	49	87	123	158	194	391	...	64848

because questions with no answers were removed. In order to avoid identifying individuals, user accounts were replaced with unique ID numbers. By using these ID numbers, we can trace any user's questions and answers in the data. Table I shows the numbers of users and their messages (questions and answers) submitted to

- PC category,
- healthcare category,
- social issues category, and
- all 286 categories in the data.

Furthermore, the following kinds of information are described in the data.

- submission time of question
- submission time of answer
- problem resolution time

Figure 1 shows an example of a series of events that occur after a questioner submits his/her question to a Q&A site. In Figure 1, the submission time of question  $q$  is  $t_q$ . Also, the submission time of answer  $a_1$  and  $a_2$  are  $t_{a1}$  and  $t_{a2}$ , respectively. Finally, the problem resolution time of question  $q$  is  $t_{pr}$ . At the problem resolution time, questioner  $Q$  stopped accepting answers and determined which answer was the best answer. We focus on time lag between answer submission and problem resolution. In case of answer  $a_2$  in Figure 1, the time lag between answer submission and problem resolution is  $t_{pr} - t_{a2}$ . The average and median of these time lags of all answers in the data of Yahoo! chiebukuro were 187595 and 64848 seconds, respectively. Table II shows the cumulative relative frequency of the time lags in the data of Yahoo! chiebukuro. As shown in Table II, in case of 1.0 percent of all answers (135705 answers), questioners stopped accepting answers and selected best answers within 87 seconds after these answers were submitted. These 135705 answers included 52798 best answers.

### B. Submissions by using multiple user accounts

There are many reasons why users in a Q&A site use multiple user accounts. First, we discuss a proper reason. In Yahoo! chiebukuro, users need not reveal their real names to submit their messages. However, their messages are traceable because their user accounts are attached to them. Because of this traceability, we can collect any user's messages and some of them include clues of identifying individuals. As a result, to avoid identifying individuals, it is reasonable and proper that users change their user accounts or use multiple user accounts. However, the following types of message submissions by using multiple user accounts are neither reasonable nor proper.

a) *TYPE QA*: One user submits a question and its answer by using multiple user accounts (Figure 2 (a)).

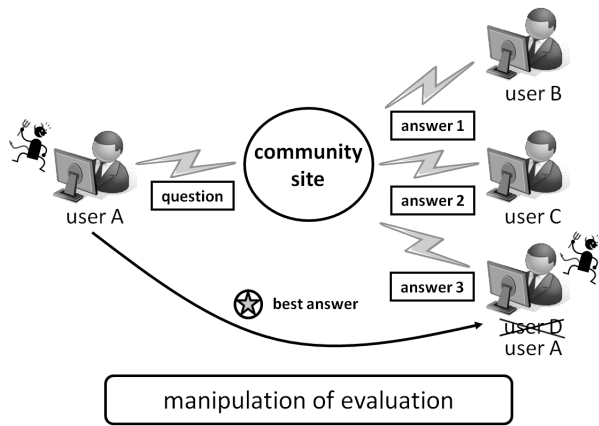
We think that the user intended to manipulate the message evaluation. For example, in Yahoo! chiebukuro, each questioner is requested to determine which answer is best and give a *best answer* label to it. These message evaluations encourage message submitters to submit new messages and increase the credibility of the Q&A site. We think that the user repeated this type of submissions because he/she wanted to get many best answer labels and be seen as a good answerer.

b) *TYPE AA*: One user submits two or more answers to the same question by using multiple user accounts (Figure 2 (b)).

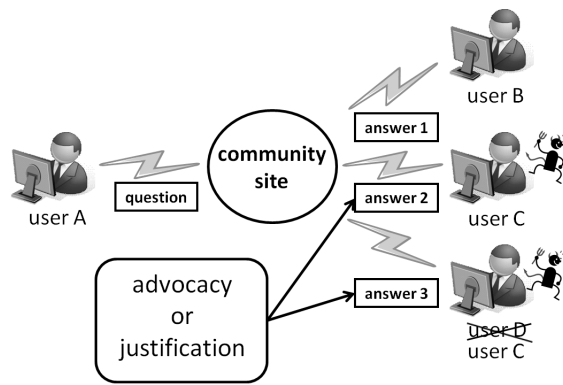
We think that the user intended to dominate or disrupt communications in the Q&A site. To be more precise, the user intended to

- control communications by advocating or justifying his/her opinions, or
- disrupt communications by submitting two or more inappropriate messages.

These two types are not all types of inadequate submissions. However, these kinds of submissions seriously disrupt communications in a Q&A site. Especially, *TYPE QA* submissions are



(a) TYPE QA: one user submits a question and its answer by using multiple user accounts. (In this case, user A submits a question and its answer by using two user accounts.)



(b) TYPE AA: one user submits two or more answers to the same question by using multiple user accounts. (In this case, user C submits two answers by using two user accounts.)

Figure 2. Two types of inadequate submissions: TYPE QA and TYPE AA.

serious because users can manipulate evaluations of messages by repeating TYPE QA submissions. Manipulated evaluations discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. To solve this problem, Watanabe et al. proposed a method of detecting users suspected of using multiple user accounts and repeating TYPE QA submissions [1]. This method was based on one idea: if a user uses multiple user accounts and attempts to manipulate his/her evaluations inadequately, the user repeats TYPE QA submissions unnaturally and gives too many good evaluations to his/her submissions. This method of inadequate submission detection was useful but not enough because there are several types of inadequate submissions. Especially, Watanabe et al.'s method did not consider when questions and answers were submitted. In order to detect inadequate submissions more widely, in this study, we focus on time lags between best answer submission and problem resolution. As mentioned, in Yahoo! chiebukuro, the median time lag between answer submission and problem resolution was 64848 seconds. However, we found some cases where time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. We think that, if a certain user

pair of questioner and answerer repeats this kind of unnatural submissions, the questioner and answerer are suspected of being one and the same user. In the next section, we propose a new method of detecting unnatural submissions by considering time lags between answer submission and problem resolution.

#### IV. UNNATURAL SUBMISSION DETECTION IN YAHOO! CHIEBUKURO

In Yahoo! chiebukuro, we found some cases where the time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. To determine whether this kind of unnatural submissions occurred, we test a hypothesis based on question and answer time lags (QAT): Hypothesis QAT. When this hypothesis is rejected by a one-sided binomial test, we determine that this kind of unnatural submissions occurred.

**Hypothesis QAT** If there are not too many cases where user  $i$  (questioner) determined that user  $j$ 's answer was the best answer just after user  $j$  (answerer) submitted it, we would expect that there are at most  $N_{QAT}(i, j, T_0)$  cases where user  $i$  determined user  $j$ 's answer was the best answer within a shorter time lag than  $T_0$ .

$$N_{QAT}(i, j, T_0) = P_{QAT}(T_0) \times ans(i, j)$$

where  $ans(i, j)$  is the total number of user  $j$ 's answers for user  $i$ 's questions and  $P_{QAT}(T_0)$  is the probability that a user answers one question randomly and the answer is selected as best answer within a shorter time lag than  $T_0$ . Because each user of Yahoo! chiebukuro can submit his/her answer only one time to one question,  $P_{QAT}(T_0)$  is

$$P_{QAT}(T_0) = \frac{N_{bestans}(T_0)}{N_{ans}}$$

where  $N_{ans}$  is the total number of answers and  $N_{bestans}(T_0)$  is the number of best answers selected within a shorter time lag than  $T_0$ . Suppose  $T_0$  was set to 87 seconds. This is because, as shown in Table II, the time lag between answer submission and problem resolution is 87 seconds when the cumulative relative frequency of answers is 0.01. When  $T_0$  is sufficiently small,  $T_0$  is independent of the categories in the data of Yahoo! chiebukuro. This is because, when  $T_0$  is sufficiently small, questioners have not enough time to read answers in any category. We think 87 seconds is sufficiently small. When  $T_0$  is sufficiently small and category-independent,  $N_{ans}$  and  $N_{bestans}(T_0)$  can be set regardless of the categories. In this study,  $N_{ans}$  was set to 13477785. It was the total number of answers in the data of Yahoo! chiebukuro (Table I). On the other hand,  $N_{bestans}(T_0)$  was set to 52798. It was the total number of best answers which were selected as best answers within 87 seconds after these best answers were submitted.

#### V. EXPERIMENTAL RESULTS

To evaluate our method, we conducted the detection of unnatural submissions in Yahoo! chiebukuro, which were suspected of being caused by multiple account users. In this experiment, the target users and submissions were all users and submissions in the data of Yahoo! chiebukuro, respectively. Also, the target categories were all 286 categories in the data of Yahoo! chiebukuro.  $T_0$  was set to 87 seconds, and then,  $N_{ans}$  and  $N_{bestans}(T_0)$  were 13477785 and 52798, respectively. The significant level of Hypothesis QAT was set to 0.000005.

This was extremely low because we intend to detect extreme unnatural submissions.

In this experiment, we tried to detect unnatural submissions in each category. Our method detected a total of 316 unnatural submissions caused by 258 user pairs. These 316 unnatural submissions can be classified into two types:

**Type A** this type of unnatural submission was caused by a user pair involved in unnatural submissions in two or more categories. For example, unnatural submissions in five categories caused by user pair (691911 ← 802184) were classified into this type. User pair (691911 ← 802184) means that user 691911 and 802184 are the questioner and answerer in this user pair, respectively. In this experiment, our method found 75 unnatural submissions of this type. These 75 unnatural submissions were caused by 17 user pairs. It is unnatural that one answerer submits answers repeatedly to the same questioner's questions in different categories. As a result, in each of these 17 user pairs, the questioner and the answerer were suspected of being one and the same user.

**Type B** this type of unnatural submission was caused by a user pair involved in unnatural submissions in only one category. In this experiment, our method found 241 unnatural submissions of this type. These 241 unnatural submissions were caused by 241 user pairs.

First, we discuss 17 user pairs involved in Type A unnatural submissions. As mentioned, these 17 user pairs were suspected. Furthermore, in questions and answers submitted by these 17 user pairs, we found many strange coincidence of opinions, mistype, expression selection, and so on. As a result, these 17 user pairs were deeply suspected. Moreover, it is notable that there were many questioners involved in Type A unnatural submissions submitted small number of answers. In the 75 type A unnatural submissions, we found 49 cases where the questioner submitted less than four answers. However, we think this is not unnatural. Suppose a questioner and answerer are one and the same user and his/her purposes is to manipulate the evaluation of the answerer. Questioner's answers are useless to manipulate the evaluation of the answerer, and consequently, the questioner submits no answer or small number of answers.

Next, we discuss user pairs involved in Type B unnatural submissions. We found suspected and unsuspected submissions in Type B unnatural submissions. In the unsuspected cases, we found five cases where the questioner and answerer used Yahoo! chiebukuro as an online chat system and communicated with each other in real time, for example,

question How can I get in touch with Mr. Kupo?  
answer Yeah! Kupo is here!!!!

After submitting this question, the questioner received eleven answers in about 20 minutes. The last answer was submitted by Kupo. The questioner selected Kupo's answer as a best answer just after he/she received it. We think a considerable number of users enjoyed realtime communication frequently in Yahoo! chiebukuro. These users could be distinguished from inadequate users when our method was used in combination with other methods, such as, similarity analysis of writing.

## VI. CONCLUSION

In order to detect unnatural submissions caused by inadequate multiple account users in a Q&A site, in this paper, we focused on time lags between answer submission and problem resolution. This is because we observed the data of Yahoo! chiebukuro, a widely-used Japanese Q&A site, and found some cases where the time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. The proposed method was based on an idea: if a user repeats submissions where the time lags between best answer submission and problem resolution are very short, the user is suspected of using multiple user accounts and attempting to manipulate his/her evaluations inadequately. In our method, unnatural submissions of this type were detected by a binomial test. We showed that our method detected many unnatural submissions. Unnatural submissions detected by our methods will give us a chance to investigate purposes and behaviors of users who use multiple user accounts and intend to manipulate evaluations in a Q&A site. We intend to combine our method with other methods, such as, similarity analysis of writing.

## REFERENCES

- [1] Y. Watanabe et al., "Investigation of users suspected of manipulating evaluations of answers in a q&a site," *International Journal on Advances in Internet Technology*, vol. 8, no. 3&4, 2015, pp. 50–63. [Online]. Available: [https://www.iariajournals.org/internet\\_technology/inttech\\_v8\\_n34\\_2015\\_paged.pdf](https://www.iariajournals.org/internet_technology/inttech_v8_n34_2015_paged.pdf) [accessed: 2018-5-1]
- [2] "Distribution of "Yahoo! Chiebukuro" data," URL: [http://www.nii.ac.jp/cscenter/idr/yahoo/tdc/chiebukuro\\_e.html](http://www.nii.ac.jp/cscenter/idr/yahoo/tdc/chiebukuro_e.html) [accessed: 2018-5-1].
- [3] A. N. Joinson, *Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives*. Palgrave Macmillan, Feb. 2003.
- [4] S. Fox et al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, The Pew Internet & American Life Project, 2000. [Online]. Available: [http://www.pewinternet.org//media/Files/Reports/2000/PIP\\_Trust\\_Privacy\\_Report.pdf](http://www.pewinternet.org//media/Files/Reports/2000/PIP_Trust_Privacy_Report.pdf) [accessed: 2016-10-4]
- [5] G. Kambourakis, "Anonymity and closely related terms in the cyberspace: An analysis by example," *Journal of Information Security and Applications*, vol. 19, no. 1, Feb. 2014, pp. 2–17. [Online]. Available: <http://dx.doi.org/10.1016/j.jisa.2014.04.001> [accessed: 2018-5-1]
- [6] J. R. Douceur, "The Sybil attack," in *Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS '02)*, Mar. 2002, pp. 251–260. [Online]. Available: <http://research.microsoft.com/pubs/74220/IPTPS2002.pdf> [accessed: 2018-5-1]
- [7] L. A. Cutillo, M. Manulis, and T. Strufe, "Security and privacy in online social networks," in *Handbook of Social Network Technologies and Applications*, B. Furht, Ed. Springer, Nov. 2010, pp. 497–522.
- [8] L. Wang and J. Kangasharju, "Real-world sybil attacks in BitTorrent mainline DHT," in *Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM 2012)*, Dec. 2012, pp. 826–832. [Online]. Available: <http://dx.doi.org/10.1109/GLOCOM.2012.6503215> [accessed: 2018-5-1]
- [9] O. de Vel, A. Anderson, M. Corney, and G. Mohay, "Mining e-mail content for author identification forensics," *SIGMOD Rec.*, vol. 30, no. 4, Dec. 2001, pp. 55–64. [Online]. Available: <http://doi.acm.org/10.1145/604264.604272> [accessed: 2018-5-1]
- [10] M. Koppel, S. Argamon, and A. Shimon, "Automatically categorizing written texts by author gender," *Literary and Linguistic Computing*, vol. 17, 2002, pp. 401–412. [Online]. Available: <https://doi.org/10.1093/lc/17.4.401> [accessed: 2018-5-1]
- [11] M. Corney, O. Y. de Vel, A. Anderson, and G. M. Mohay, "Gender-preferential text mining of e-mail discourse," in *ACSAC*, IEEE Computer Society, 2002, pp. 282–289. [Online]. Available:

- <http://dblp.uni-trier.de/db/conf/acsac/acsac2002.html> [accessed: 2018-5-1]
- [12] S. Argamon, M. Šarić, and S. S. Stein, “Style mining of electronic messages for multiple authorship discrimination: First results,” in *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '03. New York, NY, USA: ACM, 2003, pp. 475–480. [Online]. Available: <http://doi.acm.org/10.1145/956750.956805> [accessed: 2018-5-1]
- [13] R. Zheng, J. Li, H. Chen, and Z. Huang, “A framework for authorship identification of online messages: Writing-style features and classification techniques,” *Journal of the Association for Information Science and Technology*, vol. 57, no. 3, 3 2006, pp. 378–393. [Online]. Available: <http://onlinelibrary.wiley.com/doi/10.1002/asi.20316/abstract> [accessed: 2018-5-1]
- [14] A. Abbasi and H. Chen, “Visualizing authorship for identification,” in *Proceedings of 2006 IEEE International Conference on Intelligence and Security (ISI 2006)*, 2006, pp. 60–71. [Online]. Available: [http://dx.doi.org/10.1007/11760146\\_6](http://dx.doi.org/10.1007/11760146_6) [accessed: 2018-5-1]
- [15] N. Jindal and B. Liu, “Opinion spam and analysis,” in *Proceedings of the 2008 International Conference on Web Search and Data Mining (WSDM '08)*, Feb. 2008, pp. 219–230. [Online]. Available: <http://doi.acm.org/10.1145/1341531.1341560> [accessed: 2018-5-1]
- [16] G. Wu, D. Greene, B. Smyth, and P. Cunningham, “Distortion as a validation criterion in the identification of suspicious reviews,” in *Proceedings of the First Workshop on Social Media Analytics (SOMA '10)*, Jul. 2010, pp. 10–13. [Online]. Available: <http://doi.acm.org/10.1145/1964858.1964860> [accessed: 2018-5-1]
- [17] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, “Finding deceptive opinion spam by any stretch of the imagination,” in *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies (HLT '11) - Volume 1*, Jun. 2011, pp. 309–319. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2002472.2002512> [accessed: 2018-5-1]
- [18] “Amazon Mechanical Turk,” URL: <http://www.mturk.com/> [accessed: 2018-5-1].
- [19] C. Akkaya, A. Conrad, J. Wiebe, and R. Mihalcea, “Amazon Mechanical Turk for subjectivity word sense disambiguation,” in *Proceedings of the NAACL HLT 2010 Workshop on Creating Speech and Language Data with Amazon's Mechanical Turk (CSLDAMT '10)*, Jun. 2010, pp. 195–203. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1866696.1866727> [accessed: 2018-5-1]