

How “VKontakte” fake accounts influence the social network of users

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© Springer Nature Switzerland AG 2018. In this paper, the problem of fake accounts in online social networks is addressed through the lens of resulting misstatements of the structure of network interactions between users. The study of a network as a social space becomes difficult because of additional noise created by fakes. The aim of the present paper is to assess the impact of fake accounts on the characteristics of local friendship networks between users of VKontakte website in Izhevsk (Russia). The authors highlight key characteristics recognizing a fake account and present experience of the design of classifier (based on random forest algorithm) to determine the authenticity of an account. Comparison of the VKontakte network topology before and after removing the fake accounts from it shows what specific network metrics are affected by the presence of fake profiles. It was found that as the fakes are being excluded the less integrated members lose contact with most part of the network while the number of its components increases. “Fakes” serve as strong link concentrators distributed throughout the network and these fakes overestimate observed levels of assortativity and transitivity.

http://dx.doi.org/10.1007/978-3-030-02843-5_41

Keywords

Data analysis using R, Fake accounts, Online communities, Social network analysis, VKontakte

References

- [1] Adewole, K.S., Anuar, N.B., Kamsin, A., Varathan, K.D., Razak, S.A.: Malicious accounts: dark of the social networks. *J. Netw. Comput. Appl.* 79, 41–67 (2017). <https://doi.org/10.1016/j.jnca.2016.11.030>
- [2] Alymov, A.S., Baranyuk, V.V., Smirnova, O.S.: Detecting bot programs that mimic people’s behavior in the social network “VKontakte”. *Int. J. Open Inf. Technol.* 8, 55–60 (2016). (in Russian)
- [3] Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: The socialbot network: when bots socialize for fame and money. In: *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 93–102 (2011)
- [4] Cao, Q., Sirivianos, M., Yang, X., Pogueiro, T.: Aiding the detection of fake accounts in large scale social online services. In: *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, pp. 1–15 (2012)
- [5] Chen, C.-M., Guan, D., Su, Q.-K.: Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. *Inf. Sci.* 289, 133–147 (2014)
- [6] Conover, M., Ratkiewicz, J., Francisco, M., Gonçalves, B., Menczer, F., Flammini, A.: Political polarization on twitter. In: *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*, pp. 89–96 (2011)

- [7] Conti, M., Poovendran, R., Secchiero, M.: Fakebook: detecting fake profiles in on-line social networks. In: Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012), pp. 1071-1078 (2012)
- [8] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., Tesconi, M.: Fame for sale: efficient detection of fake twitter followers. *Decis. Support Syst.* 80, 56-71 (2015). <https://doi.org/10.1016/j.dss.2015.09.003>
- [9] Davydov, L.: On the use of social networks as a tool for creating political authority's image. *Int. J. Environ. Sci. Educ.* 11(18), 12423-12430 (2016)
- [10] El Azab, A., Idrees, A.M., Mahmoud, A.M., Hefny, H.: Fake account detection in twitter based on minimum weighted feature set. *Int. Sch. Sci. Res. Innov.* 10(1), 13-18 (2016)
- [11] Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A.: The rise of social bots. *Commun. ACM* 59(7), 96-104 (2016). <https://doi.org/10.1145/2818717>
- [12] Fire, M., Kagan, D., Elyashar, A., Elovici, Y.: Friend or foe? Fake profile identification in online social networks. *Soc. Netw. Anal. Min.* 4(1), 1-23 (2014)
- [13] Fire, M., Katz, G., Elovici, Y.: Strangers intrusion detection—detecting spammers and fake profiles in social networks based on topology anomalies. *ASE Hum. J.* 1(1), 26-39 (2012)
- [14] GitHub: Access to VK (Vkontakte) API via R. <https://github.com/Dementiy/vkR>. Accessed 10 Jan 2018
- [15] Top Websites Ranking. <https://www.similarweb.com/top-websites>. Accessed 10 Jan 2018
- [16] Xiao, C., Freeman, D.M., Hwa, T.: Detecting clusters of fake accounts in online social networks. In: Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, pp. 91-101 (2015). <https://doi.org/10.1145/2808769.2808779>
- [17] Yang, Z., Wilson, C., Wang, X., Gao, T., Zhao, B. Y., Dai, Y.: Uncovering social network sybils in the wild. In: Internet Measurement Conference, pp. 259-268 (2011)
- [18] Zhu, Y., Wang, X., Zhong, E., Liu, N., Li, H., Yang, Q.: Discovering spammers in social networks. In: Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, pp. 171-177 (2012)