The Information-Analytical Bots Detection System Based On The Assembly Of Classifiers

Vladimir Nikiforovich Kuzmin, Artem Bakitzhanovich Menisov and Ivan Anatolevich Shastun

November 7, 2020

The Information-Analytical Bots Detection System Based on The Assembly of Classifiers

Vladimir N. Kuzmin[0000-0002-6411-4336], Artem B. Menisov[0000-0002-9955-2694]
and Ivan A. Shastun[0000-0002-1086-5345]

Space Military Academia named by A.F.Mozhaysky,
Zhdanovskay street, 13, Saint-Petersburg, 197198, Russia
vka@mil.ru

Abstract. Currently, the use of bots, disguised as ordinary users of social networks and guidance with special programs, has serious consequences. For example, bots were used to influence political elections, distort information on the Internet, and manipulate stock prices on the stock exchange. The detection of bots in social networks is carried out by many research teams, the areas of research of which include the use of machine learning methods. However, the practical results of detecting bots on social networks indicate significant limitations, since the methodological tools used have language limitations and ineffective criteria for determining bots.

The report provides a description of the information-analytical system (client-server application) that allows for collection and analysis data of social networks in order to identify bots. The application is based on a bots detection module based on the assembly of classifiers of social network accounts, the capabilities of which allowed to minimize the risk of bot detection errors. The practical utilizing of the application allows increasing the operatively and effectiveness of detecting bots in comparison with other approaches.

Keywords: bots detection; social networks; machine learning; ensemble of models; association of classifiers.

The development of new approaches to improving the security of state organizations and users of information web-systems is a constant and urgent task.

The information-analytical system for detecting bots on social networks based on a special association of classifiers is a client-server application that allows to:

1) provide a decentralized management system, access to resources from all devices;

2) evaluate informational occasions;

3) identify bots among subscribers and in individual communities of social networks;

3) interactively display on maps and graphs the results, generate reporting and information documents;

4) provide API to third-party services.

The application is designed to improve the existing decision support system for identifying bots and developing organizational and technical measures to neutralize the consequences of using bots.

The main consumers are state and commercial organizations, as well as well-known personalities, against which negative information can be disseminated.

The connection to the server is established using the HTTPS protocol using encryption in order to increase security.

The application can be installed on any computer on the local network with any operating environment, including the Astra Linux Special Edition.

Due to the large amount of data transferred, it is necessary to have a high-speed connection between the server and the client.

To perform remote administration of the application via the web interface, the Apache webserver is required. The architecture of the application is shown in see Fig. 1.

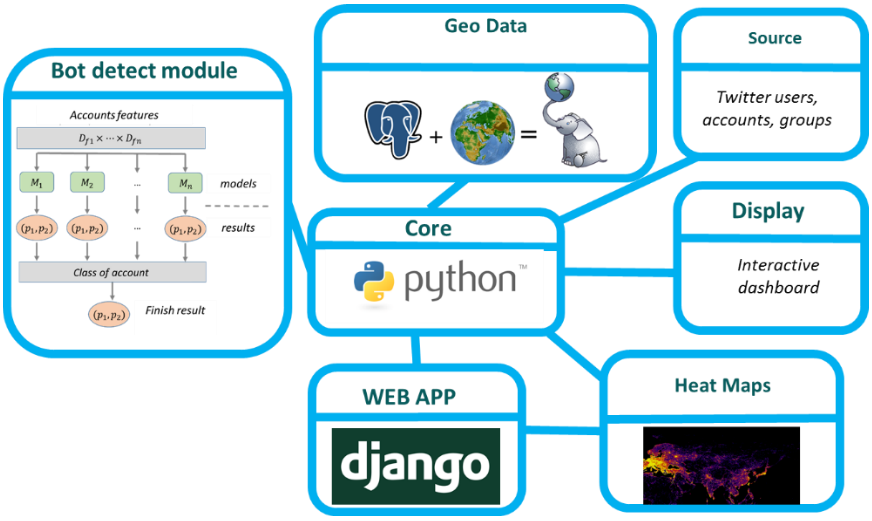

Fig. 1. The architecture of the information-analytical system for identifying bots of social networks.

An element of the scientific novelty of the developed approach for identifying bots of social networks is the recommended combination of the following features: thematic relationship of accounts, activity, anonymity, and data inconsistency. A feature of this approach is to take into account the growing tendency to use one set of bots to solve different informational goals.

The developed approach to detecting bots on the Twitter social network based on a special association of classifiers has an advantage in terms of performance over modern machine-learning algorithms and can reduce the error of detecting bots. Since the activity of social network bots includes categorical attributes, adaptation to the source, data is necessary to use ensembles of models.

However, despite the advantages of machine learning, one of the main drawbacks of the developed approach maybe its impracticality when there are too many unique records, for example, because string representations of categorical features display typos or combinations of several data in the same records.

The practical application of the application allows for increasing the efficiency and effectiveness of detecting bots in comparison with other approaches.

As a further development of research, we can distinguish:

- study of the issues of collecting additional data about social network accounts;
- analysis of the effect of data imbalance on model training;
- study of the possibilities of increasing the productivity of detecting bots of social networks.

References

1. Williamson, W., Scrofani, J.: Trends in detection and characterization of propaganda bots. In: 52nd Hawaii International Conference on System Sciences, pp. 7118 – 7123. Maui (2019).
1. Lukyanov, R.V.: Methodology for monitoring the state of information security of automated systems in the context of heterogeneous mass incidents. Transactions of the Military Space Academy named by A.F.Mozhaysky 660, 111-115 (2018).
2. As many as 48 million Twitter accounts aren’t people, says study, https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html, last accessed 2020/04/11.
3. Massive networks of fake accounts found on Twitter, http://www.bbc.co.uk/news/technology-38724082, last accessed 2020/04/11.
4. Terdima, D.: Here’s how Facebook uses AI to detect many kinds of bad content. Fast Company, https://www.fastcompany.com/40566786/heres-how-facebook-uses-ai-to-detect-many-kinds-of-bad-content, last accessed 2020/04/11
5. Fighting disinformation online. RAND, https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html, last accessed 2020/04/11.
6. Bacciu, A., La, M. M., Nemmi, E., Neri, V., Mei, A., Stefa, J.: Bot and gender detection of Twitter accounts using distortion and LSA. In: PAN at CLEF 2019 (2019).
7. Gamallo, P., Almatarneh, S.: Naïve-bayesian classification for bot detection in Twitter. In: at CLEF 2019 (2019).
8. Vogel, I., Jiang, P.: Bot and gender identification in Twitter using word and character N-grams. In: PAN at CLEF 2019 (2019).
9. Mahmood, A., Srinivasan, P.: Twitter bots and gender detection using tf-idf. In: PAN at CLEF 2019 (2019).
10. Farber, M., Qurdina, A., Ahmedi, L.: Identifying Twitter bots using a convolutional neural network. In: PAN at CLEF 2019 (2019).
11. Lundberg, J., Nordqvist, J., Laitinen, M.: Towards a language independent bot detection. In: DHN 2019, pp. 308-319. Copenhagen (2019).
12. Sahoo, S.R., Gupta, B.B.: Hybrid approach for detection of malicious profiles in Twitter. Computers & Electrical Engineering 76, 65-81 (2019).
13. Novotny, J.: Twitter bot detection & categorization - a comparative study of machine learning methods. Lund university, Lund (2019).

14. Davoudi, A., Klein, A.Z., Sarker, A., Gonzalez-Hernandez, A.: Towards automatic bot detection in Twitter for health-related tasks. Working paper ArXiv:1909.13184 (2019).
15. Mazza, M., Cresci, S., Avvenuti, M.,Quattrociocchi, W., Tesconi, M.: RTbust: Exploiting temporal patterns for dotnet detection on Twitter. In: 10th ACM Conference on Web Science, pp. 183-192. Amsterdam (2018).
16. Beskow, D.M., Carley, K.M.: Its all in a name: detecting and labeling bots by their name. Computational and Mathematical Organization Theory, 1-12 (2019).
17. Varol, O., Ferrara, E., Davis, C.A., Menczer, F., Flammini, A.: Online humanbot interactions: Detection, estimation, and characterization. In: Eleventh international AAAI conference on web and social media, https://arxiv.org/pdf/1703.03107.pdf, last accessed 2020/05/16.
18. Minnich, A., Chavoshi, N., Koutra, D., Mueen, A.: BotWalk: Efficient adaptive exploration of Twitter bot networks. In: IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, pp. 467-474 (2017).
19. Chavoshi, N., Hamooni, H., Mueen, A.: DeBot: Twitter Bot Detection via Warped Correlation. In: ICDM, pp. 817-822 (2016).
20. Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A.: The rise of social bots. Communications of the ACM. 59(7), 96-104 (2016).
21. Mazza, M., Cresci, S., Avvenuti, M., Quattrociocchi, W., Tesconi, M.: Rtbust: Exploiting temporal patterns for botnet detection on twitter, https://arxiv.org/pdf/1902.04506.pdf, last accessed 2020/05/19.
22. Twitter API Documentation, http://www.developer.twitter.com/docs, last accessed 2020/05/21.
23. Vorontsov, K.V.: Mathematical methods of teaching by procedures (theory of machine learning), http://www.machinelearning.ru, last accessed 2020/05/21.
24. Zhang, W., Du, T., Wang, J.: Deep learning over multi-field categorical data. In: European conference on information retrieval. ArXiv, abs/1601.02376. Italia, Padua (2016).
25. Menisov, A.B., Shastun, I.A., Kapitsyn, S.U.: An approach to the identification of malicious Internet sites based on the processing of lexical signs of addresses (URLs) and an average ensemble of models. Information Technologies 25(11), 691- 697 (2019).
26. Vorontsov, K.V.: Lectures on methods for evaluating and selecting models, http://www.machinelearning.ru, last accessed 2020/05/21.
27. Gorodetsky, V.I., Serebryakov, S.V.: Collective recognition methods and algorithms: a review. Transactions of SPIIRAS 1(3), 139-171 (2006).
28. Niyogi, P., Pierrot, J – B., Siohan, O.: Multiple classifiers by constrained minimization. In: International Conference on Acoustics, Speech, and Signal Processing, pp.3462-3465 Istanbul, Turkey (2000).
29. Prodromidis, A., Chan, P., Stolfo, S.: Meta-learning in distributed data mining systems: Issues and approaches. Advances in Distributed Data Mining 3, 81-114 (1999).
30. Gnidko, K.O., Makarov, S.A., Sergeev, A.S.: A model of an intellectual decision support system in order to identify the negative informational and psychological impact on students of educational organizations of the Ministry of Defense of Russia and to protect against it. Transactions of the Military Space Academy named by A.F.Mozhaysky 666, 142-147 (2019).
31. Kachura, Ya.O., Saprykin, D.I., Faleev, P.A.: Modeling of the military-political activity of states by the methods of associative analysis in decision support systems. Transactions of the Military Space Academy named by A.F.Mozhaysky 660, 19-29 (2018).