

ABSTRACT AND REFERENCES

INFORMATION TECHNOLOGY. INDUSTRY CONTROL SYSTEMS

DOI: 10.15587/1729-4061.2021.225362
DEVELOPMENT FOR PERFORMANCE OF PORTER
STEMMER ALGORITHM (p. 6–13)

Manhal Elias Polus

College of Science Al-Mustansiriyah University, Baghdad, Iraq
ORCID: <http://orcid.org/0000-0001-9168-6447>

Thekra Abbas

College of Science Al-Mustansiriyah University, Baghdad, Iraq
ORCID: <http://orcid.org/0000-0002-4435-3188>

The Porter stemmer algorithm is a broadly used, however, an essential tool for natural language processing in the area of information access. Stemming is used to remove words that add the final morphological and diacritical endings of words in English words to their root form to extract the word root, i.e. called stem/root in the primary text processing stage. In other words, it is a linguistic process that simply extracts the main part that may be close to the relative and related root. Text classification is a major task in extracting relevant information from a large volume of data. In this paper, we suggest ways to improve a version of the Porter algorithm with the aim of processing and overcome its limitations and to save time and memory by reducing the size of the words. The system uses the improved Porter derivation technique for word pruning. Whereas performs cognitive-inspired computing to discover morphologically related words from the corpus without any human intervention or language-specific knowledge. The improved Porter algorithm is compared to the original stemmer. The improved Porter algorithm has better performance and enables more accurate information retrieval (IR).

Keywords: stemming algorithm, natural language processing, information retrieval, APSA, Porter algorithm.

References

- Seddiq, H., Maruf, A. A. M., Chy, A. N. (2016). Recursive Suffix Stripping to Augment Bangla Stemmer. ICAICT-2016-Paper. Available at: [http://www.ciu.edu.bd/icaict2016/publications/ICAICT-2016-Paper%20\(50\).pdf](http://www.ciu.edu.bd/icaict2016/publications/ICAICT-2016-Paper%20(50).pdf)
- Shah, F. P., Patel, V. (2016). A review on feature selection and feature extraction for text classification. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). doi: <https://doi.org/10.1109/wispnet.2016.7566545>
- Saeed, A. M., Rashid, T. A., Mustafa, A. M., Agha, R. A. A.-R., Shamsaldin, A. S., Al-Salihi, N. K. (2018). An evaluation of Reber stemmer with longest match stemmer technique in Kurdish Sorani text classification. *Iran Journal of Computer Science*, 1 (2), 99–107. doi: <https://doi.org/10.1007/s42044-018-0007-4>
- Agbele, K., Adesina, A., Azeez, N., Abidoye, A. (2012). Context-Aware Stemming algorithm for semantically related root words. *African Journal of Computing & ICT*, 5 (4), 33–42.
- Akkus, B. K., Cakici, R. (2013). Categorization of Turkish News Documents with Morphological Analysis. 51st Annual Meeting of the Association for Computational Linguistics Proceedings of the Student Research Workshop. Sofia, 1–8. Available at: <https://www.aclweb.org/anthology/P13-3001.pdf>
- Kumar, R., Mansotra, V. (2016). Applications of stemming algorithms in information retrieval-a review. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6 (2), 418–423.
- Biba, M., Gjati, E. (2014). Boosting Text Classification through Stemming of Composite Words. *Recent Advances in Intelligent Informatics*, 185–194. doi: https://doi.org/10.1007/978-3-319-01778-5_19
- Farrar, D., Huffman Hayes, J. (2019). A Comparison of Stemming Techniques in Tracing. 2019 IEEE/ACM 10th International Symposium on Software and Systems Traceability (SST). doi: <https://doi.org/10.1109/sst.2019.00017>
- Al-Sharhan, S., Al-Hunaiyyan, A., Alhajri, R., Al-Huwail, N. (2019). Utilization of Learning Management System (LMS) Among Instructors and Students. *Advances in Electronics Engineering*, 15–23. doi: https://doi.org/10.1007/978-981-15-1289-6_2
- Joshi, A., Thomas, N., Dabhade, M. (2016). Modified Porter Stemming Algorithm. *International Journal of Computer Science and Information Technologies*, 7 (1), 266–269.

DOI: 10.15587/1729-4061.2021.225346
DEVELOPMENT OF A METHOD FOR CONSTRUCTING
LINGUISTIC STANDARDS FOR MULTI-CRITERIA
ASSESSMENT OF HONEYPOT EFFICIENCY (p. 14–23)

Anna Korchenko

National Aviation University, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0003-0016-1966>

Vladyslav Breslavskiy

Ukrainian State Centre of Radio Frequencies, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0002-9478-3442>

Serhii Yevseiev

Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: <http://orcid.org/0000-0003-1647-6444>

Nazym Zhumangalieva

Satbayev University, Almaty, Republic of Kazakhstan
 T. K. Zhurgenov Kazakh National Academy of Arts, Almaty, Republic of Kazakhstan
ORCID: <http://orcid.org/0000-0003-1130-3405>

Anatolii Zvorych

Central Scientific Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0002-7136-0295>

Svitlana Kazmirchuk

National Aviation University, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0001-6083-251X>

Oleg Kurchenko

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0002-3507-2392>

Oleksandr Laptiev

Institute of Information Protection
 State University of Telecommunications, Kyiv, Ukraine
ORCID: <http://orcid.org/0000-0002-4194-402X>

Oleksand Sievierinov

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: <http://orcid.org/0000-0002-6327-6405>

Sirhii Tkachuk

Vinnytsia National Technical University, Vinnytsia, Ukraine

ORCID: <http://orcid.org/0000-0002-7039-1233>

One of the pressing areas that is developing in the field of information security is associated with the use of Honeypots (virtual decoys, online traps), and the selection of criteria for determining the most effective Honeypots and their further classification is an urgent task. The main products that implement virtual decoy technologies are presented. They are often used to study the behavior, approaches and methods that an unauthorized party uses to gain unauthorized access to information system resources. Online hooks can simulate any resource, but more often they look like real production servers and workstations. A number of fairly effective developments are known that are used to solve the problems of detecting attacks on information system resources, which are based on the apparatus of fuzzy sets. They showed the effectiveness of the appropriate mathematical apparatus, the use of which, for example, to formalize the approach to the formation of a set of reference values that will improve the process of determining the most effective Honeypots. For this purpose, many characteristics have been formed (installation and configuration process, usage and support process, data collection, logging level, simulation level, interaction level) that determine the properties of online traps. These characteristics became the basis for developing a method for the formation of standards of linguistic variables for further selection of the most effective Honeypots. The method is based on the formation of a Honeypots set, subsets of characteristics and identifier values of linguistic estimates of the Honeypot characteristics, a base and derived frequency matrix, as well as on the construction of fuzzy terms and reference fuzzy numbers with their visualization. This will allow classifying and selecting the most effective virtual baits in the future.

Keywords: honeypot classification, virtual decoys, fuzzy standards, method of forming linguistic standards.

References

- Korchenko, A. (2019). *Metody identyfikatsii anomalnykh staniv dlia system vyivlennia vtorhnen*. Kyiv, 361.
- Stoll, C. (1990). *Cuckoo's Egg*. NY: Pocket, 356.
- Cheswick, B. (1995). *An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied*. NY: Management Analytics and Others, 147.
- Spitzner, L. (2002). *Honeypots: Tracking Hackers*. NY: Addison-Wesley Professional, 480.
- Provos, N., Holz, T. (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. NY: Addison-Wesley Professional, 440.
- Honeynet Project. Blog. Available at: <http://www.honeynet.org>
- Cohen, F., Lambert, D., Preston, C., Berry, N., Stewart, C., Thomas, E. (2001). *A Framework for Deception*. Tech. Report.
- Balas, E., Viecco, C. (2005). Towards a third generation data capture architecture for honeynets. *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005*. doi: <https://doi.org/10.1109/iaw.2005.1495929>
- Roesch, M. (1999). *Snort – lightweight intrusion detection for networks*. *Proceedings of LISA '99: 13th Systems Administration Conference*, 229–238.
- LaBrea: «Sticky» Honeypot and IDS. Available at: <http://labrea.sourceforge.net>
- Hammer, R. (2006). Enhancing IDS using, Tiny Honeypot. SANS Institute.
- The Deception Toolkit Home Page and Mailing List. The Deception Toolkit. Available at: <http://www.all.net/dtk/dtk.html>
- Baykara, M., Daş, R. (2015). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. *International Journal of Computer Networks and Applications (IJCNA)*, 2 (5), 203–211.
- Thakar, U., Varma, S., Ramani, A. (2005). *HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot*. The Second International Conference on Innovations in Information Technology (IIT'05). – Indore: Institute of Technology and Science.
- Hnatiuk, S., Volianska, V., Karpenko, S. (2012). Modern virtual decoy systems based on honeypot technology. *Ukrainian Information Security Research Journal*, 14 (3 (56)), 107–115. doi: <https://doi.org/10.18372/2410-7840.14.3398>
- Jia, Z., Cui, X., Liu, Q., Wang, X., Liu, C. (2018). *Micro-Honeypot: Using Browser Fingerprinting to Track Attackers*. 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 197–204. doi: <http://doi.org/10.1109/DSC.2018.00036>
- Park, J.-H., Choi, J.-W., Song, J.-S. (2016). *How to Design Practical Client Honeypots Based on Virtual Environment*. 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), 67–73. doi: <http://doi.org/10.1109/AsiaJCIS.2016.19>
- Almohannadi, H., Awan, I., Hamar, J. A., Cullen, A., Disso, J. P., Armitage, L. (2018). *Cyber Threat Intelligence from Honeypot Data Using Elasticsearch*. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 900–906. doi: <http://doi.org/10.1109/AINA.2018.00132>
- Fraunholz, D., Zimmermann, M., Hafner, A., Schotten, H. D. (2017). *Data Mining in Long-Term Honeypot Data*. 2017 IEEE International Conference on Data Mining Workshops (ICDMW), 649–656. doi: <http://doi.org/10.1109/ICDMW.2017.92>
- Moore, C. (2016). *Detecting Ransomware with Honeypot Techniques*. 2016 Cybersecurity and Cyberforensics Conference (CCC), 77–81. doi: <http://doi.org/10.1109/CCC.2016.14>
- Bombardieri, M., Castano, S., Curcio, F., Furfaro, A., Karatza, H. D. (2016). *Honeypot-Powered Malware Reverse Engineering*. 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), 65–69. doi: <http://doi.org/10.1109/IC2EW.2016.16>
- Lin, Y.-D., Lee, C.-Y., Wu, Y.-S., Ho, P.-H., Wang, F.-Y., Tsai, Y. L. (2014). *Active versus Passive Malware Collection*. *Computer*, 47 (4), 59–65. doi: <http://doi.org/10.1109/MC.2013.226>
- Henderson, B., Mckenna, S., Rowe, N. (2018). *Web Honeypots for Spies*. 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 1–6. doi: <http://doi.org/10.1109/CSCI46756.2018.00009>
- Kishimoto, K., Ohira, K., Yamaguchi, Y., Yamaki, H., Takakura, H. (2012). *An Adaptive Honeypot System to Capture IPv6 Address Scans*. 2012 International Conference on Cyber Security. doi: <https://doi.org/10.1109/cybersecurity.2012.28>
- Hecker, C., Hay, B. (2013). *Automated Honeynet Deployment for Dynamic Network Environment*. 2013 46th Hawaii International Conference on System Sciences. doi: <https://doi.org/10.1109/hicss.2013.110>
- Tehnologiya Honeypot. Chast' 2: Klassifikatsiya Honeypot. Available at: <https://www.securitylab.ru/analytics/275775.php>
- Honeypots primanka na hakera. Available at: <https://docplayer.ru/54222428-Honeypots-primanka-na-hakera.html>
- Kotenko, I. V., Stepashkin, M. V. (2014). *Deception systems for protection of information resources in computer networks*. *SPIIRAS Proceedings*, 1 (2), 211. doi: <https://doi.org/10.15622/sp.2.16>

29. Korchenko, O. H., Kazmirchuk, S. V., Akhmetov, B. B. (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiynoi bezpeky. Kyiv, 435.
30. Korchenko, A. G. (2006). The development of information protection systems based on the fuzzy sets. The theory and practical solutions. Kyiv, 320.
31. Korchenko, A. A. (2014). Metod formirovaniya lingvisticheskikh etalonov dlya sistem vyyavleniya vtorzheniy. Zakhyst informatsiyi, 16 (1), 5–12.
32. Akhmetov, B., Korchenko, A., Akhmetova, S., Zhumangalieva, N. (2016). Improved method for the formation of linguistic standards for of intrusion detection systems. Journal of Theoretical and Applied Information Technology, 87 (2), 221–232.
33. Zhumangaliyeva, N., Doszhanova, A., Korchenko, A., Kazmirchuk, S., Avkurova, Z., Zhaxygulova, D. (2020). Method of linguistic variable standards formation for honeypot classification. Bulletin of national academy of sciences of the republic of Kazakhstan, 5 (387), 16–24. doi: <https://doi.org/10.32014/2020.2518-1467.138>
34. Zhumangaliyeva, N., Korchenko, A., Doszhanova, A., Shaikhanova, A., Zhadyra, S. G. A. (2019). Detection environment formation method for anomaly detection systems. Journal of Theoretical and Applied Information Technology, 97 (16), 4239–4250.
35. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., Kozak, R. (2017). The etalon models of linguistic variables for sniffing-attack detection. 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: <https://doi.org/10.1109/idaacs.2017.8095087>
36. Korchenko, A., Warwas, K., Klos-Witkowska, A. (2015). The tuple model of basic components' set formation for cyberattacks. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: <https://doi.org/10.1109/idaacs.2015.7340782>

DOI: 10.15587/1729-4061.2021.225339

DEVELOPMENT OF AN ALGORITHM TO PROTECT USER COMMUNICATION DEVICES AGAINST DATA LEAKS (p. 24–33)

Alexander Zadereyko

National University “Odessa Law Academy”, Odessa, Ukraine
ORCID: <http://orcid.org/0000-0003-0497-9861>

Yuliia Prokop

O. S. Popov Odessa National Academy of Telecommunications,
 Odessa, Ukraine
ORCID: <http://orcid.org/0000-0002-6608-3668>

Olena Trofymenko

National University “Odessa Law Academy”, Odesa, Ukraine
ORCID: <http://orcid.org/0000-0001-7626-0886>

Natalia Loginova

National University “Odessa Law Academy”, Odesa, Ukraine
ORCID: <http://orcid.org/0000-0002-9475-6188>

Olha Plachinda

Odessa National Polytechnic University, Odessa, Ukraine
ORCID ID: <http://orcid.org/0000-0003-3382-229X>

In order to identify ways used to collect data from user communication devices, an analysis of the interaction between DNS customers and the Internet name domain space has been carried out. It has been established that the communication device's DNS traffic

is logged by the DNS servers of the provider, which poses a threat to the privacy of users. A comprehensive algorithm of protection against the collection of user data, consisting of two modules, has been developed and tested. The first module makes it possible to redirect the communication device's DNS traffic through DNS proxy servers with a predefined anonymity class based on the proposed multitest. To ensure a smooth and sustainable connection, the module automatically connects to a DNS proxy server that has minimal response time from those available in the compiled list. The second module blocks the acquisition of data collected by the developers of the software installed on the user's communication device, as well as by specialized Internet services owned by IT companies. The proposed algorithm makes it possible for users to choose their preferred level of privacy when communicating with the Internet space, thereby providing them with a choice of privacy level and, as a result, limiting the possibility of information manipulation over their owners. The DNS traffic of various fixed and mobile communication devices has been audited. The analysis of DNS traffic has enabled to identify and structure the DNS requests responsible for collecting data from users by the Internet services owned by IT companies. The identified DNS queries have been blocked; it has been experimentally confirmed that the performance of the basic and application software on communication devices was not compromised.

Keywords: DNS query, DNS server, DNS leaks, DNS traffic, DNS proxy server, data collection.

References

1. Garcia-Dorado, J. L., Ramos, J., Rodriguez, M., Aracil, J. (2018). DNS weighted footprints for web browsing analytics. Journal of Network and Computer Applications, 111, 35–48. doi: <http://doi.org/10.1016/j.jnca.2018.03.008>
2. Guelke, J. (2020). Leaking. International Encyclopedia of Ethics, 6, 1–7. doi: <http://doi.org/10.1002/9781444367072.wbiee898>
3. Trish, B. (2018). Big Data under Obama and Trump: The Data-Fueled U.S. Presidency. Politics and Governance, 6 (4), 29–39. doi: <http://doi.org/10.17645/pag.v6i4.1565>
4. Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law, 7 (1), 36–47. doi: <http://doi.org/10.1093/idpl/1pw026>
5. Google: зловещая черта (2019). Available at: <https://eurasia.film/2019/08/google-v-tvoej-golove/>
6. Saeli, S., Bisio, E., Lombardo, P., Massa, D. (2020). DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach. International Conference on Malicious and Unwanted Software (MALWARE), 46–55. Available at: https://www.researchgate.net/publication/344485984_DNS_Covert_Channel_Detection_via_Behavioral_Analysis_a_Machine_Learning_Approach
7. Chen, X., Navidi, T., Rajagopal, R. (2020). Generating private data with user customization. Available at: https://www.researchgate.net/publication/346614406_Generating_private_data_with_user_customization
8. Liu, X., Li, H., Lu, X., Xie, T., Mei, Q., Feng, F., Mei, H. (2018). Understanding Diverse Usage Patterns from Large-Scale App-store-Service Profiles. IEEE Transactions on Software Engineering, 44 (4), 384–411. doi: <http://doi.org/10.1109/tse.2017.2685387>
9. Stachl, C., Au, Q., Schoedel, R., Gosling, S. D., Harari, G. M., Buschek, D. et. al. (2020). Predicting personality from patterns of behavior collected with smartphones. Proceedings of the National Academy of Sciences, 117 (30), 17680–17687. doi: <http://doi.org/10.1073/pnas.1920484117>

10. Waheed, H., Anjum, M., Rehman, M., Khawaja, A. (2017). Investigation of user behavior on social networking sites. *PLOS ONE*, 12 (2), e0169693. doi: <http://doi.org/10.1371/journal.pone.0169693>
11. Zadereyko, O., Trofymenko, O., Loginova, N. (2019). Algorithm of user's personal data protection against data leaks in Windows 10 OS. *Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska*, 9 (1), 41–44. doi: <http://doi.org/10.5604/01.3001.0013.0905>
12. Raber, F., Vossebein, N. (2017). URetail: Privacy User Interfaces for Intelligent Retail Stores. *Human-Computer Interaction INTERACT 2017. Lecture Notes in Computer Science*. Cham: Springer, 10516, 473–477. doi: http://doi.org/10.1007/978-3-319-68059-0_54
13. Siby, S., Juarez, M., Diaz, C., Narseo, V., Troncoso, C. (2019). Encrypted DNS – Privacy? A Traffic Analysis Perspective. *Cryptography and Security*, 1–19. Available at: <https://arxiv.org/abs/1906.09682>
14. Grothoff, C., Wachs, M., Ermert, M., Appelbaum, J. (2018). Toward secure name resolution on the internet. *Computers & Security*, 77, 694–708. doi: <http://doi.org/10.1016/j.cose.2018.01.018>
15. Bumanglag, K., Kettani, H. (2020). On the Impact of DNS Over HTTPS Paradigm on Cyber Systems. 3rd International Conference on Information and Computer Technologies (ICICT). San Jose, 494–499. doi: <http://doi.org/10.1109/iciict50521.2020.00085>
16. Yan, Z., Lee, J.-H. (2020). The road to DNS privacy. *Future Generation Computer Systems*, 112, 604–611. doi: <http://doi.org/10.1016/j.future.2020.06.012>
17. Imana, B., Korolova, A., Heidemann, J. (2018). Enumerating Privacy Leaks in DNS Data Collected Above the Recursive. *Proceedings of the ISOC NDSS Workshop on DNS Privacy*. San Diego, 1–7. Available at: <https://www.isi.edu/~johnh/PAPERS/Imana18a.pdf>
18. Hoang, N., Niaki, A., Borisov, N., Gill, P., Polychronakis, M. (2020). Assessing the Privacy Benefits of Domain Name Encryption. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*. New York, 290–304. doi: <http://doi.org/10.1145/3320269.3384728>
19. Deccio, C., Davis, J. (2019). DNS privacy in practice and preparation. *Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies (CoNEXT'19)*, 138–143. doi: <http://doi.org/10.1145/3359989.3365435>
20. Beliavskii, D. (2015). DNS: kto ne spriatalsia, tot i vinovat. *Internet v tsifrakh*, 1 (21), 74–77. Available at: <http://37.230.117.45/upload/iblock/690/6900620c7bef412cfa870a549817b4fd.pdf>
21. Houser, R., Li, Zh., Cotton, Ch., Wang, H. (2019). An investigation on information leakage of DNS over TLS. *Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies (CoNEXT'19)* New York, 123–137. doi: <http://doi.org/10.1145/3359989.3365429>
22. Borgolte, K., Chattopadhyay, T., Feamster, N., Kshirsagar, M., Holland, J., Hounsel, A., Schmitt, P. (2019). How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. *SSRN Electronic Journal*. doi: <http://doi.org/10.2139/ssrn.3427563>
23. Rai, T., Verma, R. (2015). Packet Filtering Technique for Network Security. *International Journal of Engineering Research & Technology (IJERT)*, 3 (20), 1–3. Available at: <https://www.ijert.org/research/packet-filtering-technique-for-network-security-IJERT-CONV3IS20047.pdf>
24. Sheluhin, O. I., Smychek, M. A., Simonyan, A. G. (2018). Filtering unwanted applications of Internet resources for information security purposes. *H&ES Research*, 10 (2), 87–98. Available at: <https://www.elibrary.ru/item.asp?id=34939631>
25. Smart DNS Proxy Servers. Available at: <https://www.smartdnsproxy.com/Servers>
26. Podkorytov, D., Floka, A., Kuleshov S. (2019). Arkhitektura krossplatformennogo DNS Proxy servisa. *T-Comm: Telekomunikatsii i transport*, 13 (5), 35–40. Available at: https://www.researchgate.net/publication/333844552_Podkorytov_DA_Floka_AB_Kulesov_SV_Arhitektura_krossplatformennogo_DNS_Proxy_servisa_T-Comm_Telekommunikacii_i_transport_2019_Tom_13_No5_S_35-40
27. Dooley, M., Rooney, T. (2020). Navigating the Internet with DNS. *IP Address Management*, 75–92. doi: <http://doi.org/10.1002/9781119692263.ch4>
28. Fujiwara, K., Sato, A., Yoshida, K. (2019). Cache Effect of Shared DNS Resolver. *IEICE Transactions on Communications*, E102.B (6), 1170–1179. doi: <http://doi.org/10.1587/transcom.2018ebp3184>
29. General Data Protection Regulation (EU GDPR). Available at: <https://gdpr-text.com/>
30. Charanjeet, S. (2020). How to Enable DNS Over HTTPS in Chrome, Firefox, Edge, Brave & More? *Fossbytes*. Available at: <https://fossbytes.com/how-to-enable-dns-over-https-on-chrome-firefox-edge-brave/>
31. Ashok, A., John, A., Joy, P., Vijayan, R., Amrutha, V., Deepa, K., Jooby, E. (2016). Proxy Server Protection for Web Search. *International Journal of Computer Science and Technology*, 7 (1), 165–169. Available at: <http://www.ijcst.com/vol71/2/34-amrutha-ashok.pdf>
32. Shima, K., Nakamura, R., Okada, K., Ishihara, T., Miyamoto, D., Sekiya, Y. (2019). Classifying DNS Servers Based on Response Message Matrix Using Machine Learning. *International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, 1550–1551. doi: <http://doi.org/10.1109/csci49370.2019.00291>

DOI: 10.15587/1729-4061.2021.225383

OPTIMAL PARAMETER VALUES OF PID CONTROLLER FOR DC MOTOR BASED ON MODIFIED PARTICLE SWARM OPTIMIZATION WITH ADAPTIVE INERTIA WEIGHT (p. 35–45)

Mohammed Obaid Mustafa

College of Engineering University of Mosul, Mosul, Iraq

ORCID: <http://orcid.org/0000-0001-5188-6508>

A significant problem in the control field is the adjustment of PID controller parameters. Because of its high nonlinearity property, control of the DC motor system is difficult and mathematically repetitive. The particle swarm optimization PSO solution is a great optimization technique and a promising approach to address the problem of optimum PID controller results. In this paper, a modified particle swarm optimization PSO method with four inertia weight functions is suggested to find the global optimum parameters of the PID controller for speed and position control of the DC motor. Benchmark studies of inertia weight functions are described. Two scenarios have been suggested in order to modify PSO including the first scenario called M1-PSO and the second scenario called M2-PSO, as well as classical PSO algorithms. For the first scenario, the modification of the PSO was done based on changing the four inertia weight functions, social and personal acceleration coefficient, while in the second scenario, the four inertia weight functions have been changed but the social and personal acceleration coefficient stayed constant during the algorithm implementation. The comparison between the presented scenarios and traditional PID was carried out and satisfied simulation results have shown that the first scenario has rapid search speeds, and very

effective and fast implementation compared to the second scenario and classical PSO and even improved PSO technique. Moreover, the proposed approach has a fast searching speed compared to classical PSO. However, it has been found that the classical PSO algorithm has a premature, inaccurate and local convergence process when solving complex optimization issues. The presented algorithm is proposed to increase the search speed of the original PSO.

Keywords: tuning of PID, particle swarm optimization, DC motor, inertia weight functions.

References

- De la Guerra, A., Alvarez-Icaza, L., Torres, L. (2018). Brushless DC motor control with unknown and variable torque load. *IFAC-PapersOnLine*, 51 (13), 644–649. doi: <https://doi.org/10.1016/j.ifacol.2018.07.353>
- Åström, K. J., Hägglund, T. (2001). The future of PID control. *Control Engineering Practice*, 9 (11), 1163–1175. doi: [https://doi.org/10.1016/s0967-0661\(01\)00062-4](https://doi.org/10.1016/s0967-0661(01)00062-4)
- Leena, N., Shanmugasundaram, R. (2014). Artificial neural network controller for improved performance of brushless DC motor. 2014 International Conference on Power Signals Control and Computations (EPSCICON). doi: <https://doi.org/10.1109/epsicon.2014.6887513>
- Azman, M. A. H., Aris, J. M., Hussain, Z., Samat, A. A. A., Nazelan, A. M. (2017). A comparative study of fuzzy logic controller and artificial neural network in speed control of separately excited DC motor. 2017 7th IEEE International Conference on Control System, Computing and Engineering (ICCSCE). doi: <https://doi.org/10.1109/iccsce.2017.8284430>
- Bennett, S. (2001). The past of PID controllers. *Annual Reviews in Control*, 25, 43–53. doi: [https://doi.org/10.1016/s1367-5788\(01\)00005-0](https://doi.org/10.1016/s1367-5788(01)00005-0)
- Bennett, S. (1993). Development of the PID controller. *IEEE Control Systems*, 13(6), 58–62. doi: <https://doi.org/10.1109/37.248006>
- Fišer, J., Zitek, P. (2019). PID Controller Tuning via Dominant Pole Placement in Comparison with Ziegler-Nichols Tuning. *IFAC-PapersOnLine*, 52 (18), 43–48. doi: <https://doi.org/10.1016/j.ifacol.2019.12.204>
- Åström, K. J., Hägglund, T. (2004). Revisiting the Ziegler–Nichols step response method for PID control. *Journal of Process Control*, 14(6), 635–650. doi: <https://doi.org/10.1016/j.jprocont.2004.01.002>
- Åström, K., Hägglund, T. (1995). PID controllers: theory, design, and tuning. Research Triangle Park.
- Mishra, A. K., Tiwari, V. K., Kumar, R., Verma, T. (2013). Speed control of dc motor using artificial bee colony optimization technique. 2013 International Conference on Control, Automation, Robotics and Embedded Systems (CARE). doi: <https://doi.org/10.1109/care.2013.6733772>
- Rodríguez-Molina, A., Villarreal-Cervantes, M. G., Aldape-Pérez, M. (2017). An adaptive control study for a DC motor using metaheuristic algorithms. *IFAC-PapersOnLine*, 50 (1), 13114–13120. doi: <https://doi.org/10.1016/j.ifacol.2017.08.2164>
- Syafaah, L., Widiyanto, Pakaya, I., Suhardi, D., Irfan, M. (2017). PID designs using DE and PSO algorithms for damping oscillations in a DC motor speed. 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). doi: <https://doi.org/10.1109/eeesi.2017.8239138>
- Potnuru, D., Alice Mary, K., Sai Babu, C. (2019). Experimental implementation of Flower Pollination Algorithm for speed controller of a BLDC motor. *Ain Shams Engineering Journal*, 10 (2), 287–295. doi: <https://doi.org/10.1016/j.asej.2018.07.005>
- Taki El-Deen, A., Mahmoud, A. A. H., R. El-Sawi, A. (2015). Optimal PID Tuning for DC Motor Speed Controller Based on Genetic Algorithm. *International Review of Automatic Control (IREACO)*, 8 (1), 80. doi: <https://doi.org/10.15866/ireaco.v8i1.4839>
- Mamchur, D., Yatsiuk, R. (2018). Development of the PID-neuro-controller to compensate for the impact of damages and degradation of induction motor on operation of the electric drive system. *Eastern-European Journal of Enterprise Technologies*, 5 (2 (95)), 66–77. doi: <https://doi.org/10.15587/1729-4061.2018.136466>
- Muniraj, M., Arulmozhiyal, R., Kesavan, D. (2020). An Improved Self-tuning Control Mechanism for BLDC Motor Using Grey Wolf Optimization Algorithm. *International Conference on Communication, Computing and Electronics Systems*, 315–323. doi: https://doi.org/10.1007/978-981-15-2612-1_30
- Achanta, R. K., Pamula, V. K. (2017). DC motor speed control using PID controller tuned by jaya optimization algorithm. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). doi: <https://doi.org/10.1109/icpsi.2017.8391856>
- Qi, Z., Shi, Q., Zhang, H. (2020). Tuning of Digital PID Controllers Using Particle Swarm Optimization Algorithm for a CAN-Based DC Motor Subject to Stochastic Delays. *IEEE Transactions on Industrial Electronics*, 67 (7), 5637–5646. doi: <https://doi.org/10.1109/tie.2019.2934030>
- Xie, W., Wang, J.-S., Wang, H.-B. (2019). PI Controller of Speed Regulation of Brushless DC Motor Based on Particle Swarm Optimization Algorithm with Improved Inertia Weights. *Mathematical Problems in Engineering*, 2019, 1–12. doi: <https://doi.org/10.1155/2019/2671792>
- Agarwal, J., Parmar, G., Gupta, R. (2018). Comparative Analysis of PID Controller for Speed Control of DC motor with Intelligent Optimization Algorithms. 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 273–277. doi: <https://doi.org/10.1109/icaccn.2018.8748475>
- Gupta, S., Deep, K. (2019). A novel hybrid sine cosine algorithm for global optimization and its application to train multilayer perceptrons. *Applied Intelligence*, 50 (4), 993–1026. doi: <https://doi.org/10.1007/s10489-019-01570-w>
- Hashim, N. L. S., Yahya, A., Andromeda, T., Kadir, M. R. R. A., Mahmud, N., Samion, S. (2012). Simulation of PSO-PI Controller of DC Motor in Micro-EDM System for Biomedical Application. *Procedia Engineering*, 41, 805–811. doi: <https://doi.org/10.1016/j.proeng.2012.07.247>
- Kennedy, J., Eberhart, R. (1995). Particle Swarm Optimization. *Proceedings of ICNN'95 - International Conference on Neural Networks*, 1942–1948. doi: <https://doi.org/10.1109/icnn.1995.488968>
- Shi, Y., Eberhart, R. (1998). A modified particle swarm optimizer. 1998 IEEE International Conference on Evolutionary Computation Proceedings. *IEEE World Congress on Computational Intelligence (Cat. No.98TH8360)*. doi: <https://doi.org/10.1109/icc.1998.699146>
- Zhan, Z.-H., Zhang, J., Li, Y., Chung, H. S.-H. (2009). Adaptive Particle Swarm Optimization. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 39 (6), 1362–1381. doi: <https://doi.org/10.1109/tsmcb.2009.2015956>

DOI: 10.15587/1729-4061.2021.225517

THE SYNTHESIS OF CONTROL SYSTEM TO SYNCHRONIZE SHIP GENERATOR ASSEMBLIES (p. 45–63)

Vitalii Budashko

National University «Odessa Maritime Academy», Odessa, Ukraine
ORCID: <http://orcid.org/0000-0003-4873-5236>

Valerii Shevchenko

Training & Certifying Center of Seafarers National University
«Odessa Maritime Academy», Odessa, Ukraine
ORCID: <http://orcid.org/0000-0003-3229-1909>

This paper considers the construction of principles and the synthesis of a system of effective control over the processes of synchronization of generator sets (GSs) that form a part of the distributed MP-control systems for complex ship technical systems and complexes (STS and C). The tasks of synchronization have been set, the process and database models have been built, the system configurations have been defined. Based on the use of resultant functions, we have determined stages in solving the tasks of control over the frequency adjustment synchronization in a hierarchical sequence. The performance analysis of the STS and C control elements has been carried out; the use of the integrated optimization criteria and dual management principles has been proposed. Practical techniques to manage the GS synchronization have been given. We have solved the problem of high-speed control over the frequency of synchronized objects based on the principles of adjustment. That has made it possible to determine in advance the moments of GS enabling under the deterministic and stochastic statement of the synchronization task. The results of the experimental study into the GS synchronization processes are given; the effectiveness of the proposed GS control has been proven. The principles underlying the construction of procedures to control the GS composition when using the methods of “rigid” and “flexible” thresholds have made it possible to define the optimization criteria and implement a control law that satisfied the condition for an extremum, which is an indicator of the feasibility of the set goal and takes into consideration the limitations of control influences. We managed to design a system in the class of adaptive control systems by the appropriate decomposition of the system’s elements by splitting a synchronization task into the task on performance and the task on control under the required conditions. The given examples of the processes where the synchronization failed while using standard synchronizer control algorithms, as well as processes of successful GS synchronization when applying the proposed synchronizer dual control algorithms, have confirmed the reliability of the main scientific results reported here.

Keywords: technical operation, synchronization, quality, control system, mathematical modeling.

References

- Boveri, A., Silvestro, F., Gualeni, P. (2016). Ship electrical load analysis and power generation optimisation to reduce operational costs. 2016 International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference (ESARS-ITEC). doi: <https://doi.org/10.1109/esars-itec.2016.7841422>
- Shevchenko, V. A. (2018). Optimization of the process of automatic synchronization of ship diesel generators in the deterministic formulation of the problem. Automation of technological and business processes, 10 (4), 43–53. doi: <https://doi.org/10.15673/atbp.v10i4.1233>
- Pipchenko, A. N., Ponomarenko, V. V., Teplov, Yu. I., Shevchenko, V. A. (2019). Elektrooborudovanie, elektronnaya apparatura i sistemy upravleniya. Odessa: TES, 567.
- Carrión, M., Zárate-Miñano, R., Milano, F. (2020). Impact of off-nominal frequency values on the generation scheduling of small-size power systems. International Journal of Electrical Power & Energy Systems, 122, 106174. doi: <https://doi.org/10.1016/j.ijepes.2020.106174>
- Ghaedi, A., Golshan, M. E. H. (2021). Modified WLS three-phase state estimation formulation for fault analysis considering measurement and parameter errors. Electric Power Systems Research, 190, 106854. doi: <https://doi.org/10.1016/j.epsr.2020.106854>
- Xu, F., Yang, W., Li, H. (2020). Computation offloading algorithm for cloud robot based on improved game theory. Computers & Electrical Engineering, 87, 106764. doi: <https://doi.org/10.1016/j.compeleceng.2020.106764>
- Heinrich, B., Krause, F., Schiller, A. (2019). Automated planning of process models: The construction of parallel splits and synchronizations. Decision Support Systems, 125, 113096. doi: <https://doi.org/10.1016/j.dss.2019.113096>
- Kumar, J., Kumpulainen, L., Kauhaniemi, K. (2019). Technical design aspects of harbour area grid for shore to ship power: State of the art and future solutions. International Journal of Electrical Power & Energy Systems, 104, 840–852. doi: <https://doi.org/10.1016/j.ijepes.2018.07.051>
- Chen, H. (2020). Simulation Research on Ship Electric Propulsion Speed Regulation System Based on Variable Structure Control and FPGA. Microprocessors and Microsystems, 103588. doi: <https://doi.org/10.1016/j.micpro.2020.103588>
- Aiello, G., Giallanza, A., Vacante, S., Fasoli, S., Mascarella, G. (2020). Propulsion Monitoring System for Digitized Ship Management: Preliminary Results from a Case Study. Procedia Manufacturing, 42, 16–23. doi: <https://doi.org/10.1016/j.promfg.2020.02.018>
- Attia, A.-F., Sharaf, A. M. (2020). A robust FACTS based fuzzy control scheme for dynamic stabilization of generator station. Ain Shams Engineering Journal, 11 (3), 629–641. doi: <https://doi.org/10.1016/j.asej.2019.11.004>
- Emam, S. E. A. (2004). Automatic digital synchronization. International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC '04, 778–784. doi: <https://doi.org/10.1109/iceec.2004.1374594>
- Guzzella, L., Onder, C. H. (2010). Introduction to Modeling and Control of Internal Combustion Engine Systems. Springer. doi: <https://doi.org/10.1007/978-3-642-10775-7>
- Mi, Y., Xu, Y., Lang, Z., Yang, X., Ge, X., Fu, Y., Jin, C. (2021). The frequency-voltage stability control for isolated wind-diesel hybrid power system. Electric Power Systems Research, 192, 106984. doi: <https://doi.org/10.1016/j.epsr.2020.106984>
- Myrhorod, V., Hvozdeva, I., Budashko, V. (2020). Multi-parameter Diagnostic Model of the Technical Conditions Changes of Ship Diesel Generator Sets. 2020 IEEE Problems of Automated Electrodrive. Theory and Practice (PAEP). doi: <https://doi.org/10.1109/paep49887.2020.9240905>
- Sadeghian, Z., Akbari, E., Nematzadeh, H. (2021). A hybrid feature selection method based on information theory and binary butterfly optimization algorithm. Engineering Applications of Artificial Intelligence, 97, 104079. doi: <https://doi.org/10.1016/j.engappai.2020.104079>
- Shevchenko, V. A. (2018). Ships electrical power plant control system top level algorithm synthesis method and specifics. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 6 (247), 165–174.
- Boyko, A., Budashko, V., Yushkov, Y., Boyko, N. (2016). Synthesis and research of automatic balancing system of voltage converter fed induction motor currents. Eastern-European Journal of Enterprise Technologies, 1 (2 (79)), 22–34. doi: <https://doi.org/10.15587/1729-4061.2016.60544>
- Budashko, V., Shevchenko, V. (2018). Synthesis of the Management Strategy of the Ship Power Plant for the Combined Propulsion Complex. 2018 IEEE 5th International Conference on Methods and

- Systems of Navigation and Motion Control (MSNMC). doi: <https://doi.org/10.1109/msnmc.2018.8576266>
20. Budashko, V. (2020). Thrusters Physical Model Formalization With Regard to Situational and Identification Factors of Motion Modes. *International Journal of Energy and Environment*, 14, 5–8. doi: <https://doi.org/10.46300/91012.2020.14.2>
 21. Karatas, B. C., Sarkar, M., Jóhannsson, H., Nielsen, A. H., Sørensen, P. E. (2020). Voltage stability assessment accounting for current-limited converters. *Electric Power Systems Research*, 189, 106772. doi: <https://doi.org/10.1016/j.epsr.2020.106772>
 22. Kowalski, J., Krawczyk, B., Woźniak, M. (2017). Fault diagnosis of marine 4-stroke diesel engines using a one-vs-one extreme learning ensemble. *Engineering Applications of Artificial Intelligence*, 57, 134–141. doi: <https://doi.org/10.1016/j.engappai.2016.10.015>
 23. Luo, T., Zhang, L., Zhang, C., Ma, J., Xu, Z., Sun, X., Zhao, S. (2018). Role of water as the co-solvent in eco-friendly processing oil extraction: Optimization from experimental data and theoretical approaches. *Chemical Engineering Science*, 183, 275–287. doi: <https://doi.org/10.1016/j.ces.2018.03.015>
 24. Motienko, A. (2020). Integration of information and communication system for public health data collection and intelligent transportation system in large city. *Transportation Research Procedia*, 50, 466–472. doi: <https://doi.org/10.1016/j.trpro.2020.10.055>
 25. Nuchturee, C., Li, T., Xia, H. (2020). Energy efficiency of integrated electric propulsion for ships – A review. *Renewable and Sustainable Energy Reviews*, 134, 110145. doi: <https://doi.org/10.1016/j.rser.2020.110145>
 26. Pakshina, N. A., Pravdina, M. V., Koposov, A. S., Pakshin, P. V. (2017). Team Public Testing in Classroom Studies on Automatic Control Theory. *IFAC-PapersOnLine*, 50 (1), 13468–13473. doi: <https://doi.org/10.1016/j.ifacol.2017.08.2318>
 27. Pipchenko, A. D., Shevchenko, V. A. (2018). Vessel heading robust automatic controller for varying conditions. *Marine Intellectual Technologies*, 4 (4 (42)), 208–214.
 28. Gaysarov, R. V. (2005). Rezhimy raboty elektrooborudovaniya elektricheskikh stantsiy i podstantsiy: Chast' 1. Rezhimy raboty sinhronnyh generatorov i kompensatorov. Konspekt lektsiy. Chelyabinsk: Izd-vo YuUrGU, 42.
 29. Dorogan', O. I. (2013). Mikroprotsessornye sredstva upravleniya parallel'noy rabotoy dizel'-generatornyh agregatov. *Mater. Vseukr. nauk.-tekhn. konf. z mizhnarodnoiu uchastiu. Mykolaiv*, 3–7.
 30. Zaharchenko, V. N., Shevchenko, V. A. (2015). Reshenie zadach upravleniya sudovoy elektroenergeticheskoy ustanovkoy pri izmenenii nagruzki. *Sudovye energeticheskie ustanovki*, 36, 74–82.
 31. Kut'yashova, A. Yu. (2011). Uovershenstvovanie sistem sbora i otobrazheniya informatsii na energoobektah. *Sbornik dokl. 3-y vseross. konf. «Rekonstruktsiya energetiki – 2011»*. Moscow: OOO «Intehko», 81–85.
 32. Pavlenko, M. A., Rudenko, V. N., Berdnik, P. G., Danyuk, Y. V. (2010). Systems of support of making a decision and task of their ergonomic planning. *Military Technical Collection*, 3, 3–7. doi: <https://doi.org/10.33577/2312-4458.3.2010.3-7>
 33. Pavlov, G. M., Merkur'ev, G. V. (2015). *Avtomatika energosistem. NOU "Tsentr podgotovki kadrov energosistem"*. Sankt-Peterburg. Available at: <https://rza.org.ua/down/open/Avtomatika-energostem--G-M--Pavlov--G-V--Merkurev.html>
 34. Dorohan', O. I. (2013). Pat. No. 82745 UA. Functional structure of logical-dynamic synchronization process of generator and network. No. u201300569; declared: 17.01.2013; published: 12.08.2013.
 35. Riabenkyi, V. M., Ushkarenko, O. O., Dorohan, O. I., Babak, V. I. (2013). Pat. No. 82749 UA. Method for conversion of analogue generator signal in logical-dynamic process of synchronization thereof with network. No. u201300575; declared: 17.01.2013; published: 12.08.2013.
 36. Savenko, O. Ye. (2013). Optimization of the ship's power plant to improve the quality of electricity. *Visnyk of Vinnytsia Polytechnical Institute*, 6, 74–78.
 37. Savenko, O. Ye. (2011). Theoretical and experimental study of the multigenerating ship power system functioning. *Visnyk of Vinnytsia Polytechnical Institute*, 3, 58–62.
 38. Tykhonov, I. V., Davydov, V. S., Kucheruk, S. M., Bohomia, V. I. (2013). *Osnovy teorii pokhybok vymiriuvan*. Kyiv, 66.

DOI: 10.15587/1729-4061.2021.225362**УДОСКОНАЛЕННЯ АЛГОРИТМУ СТЕММЕР ПОРТЕРА (с. 6–13)****Manhal Elias Polus, Thekra Abbas**

Алгоритм стеммер Портера є широко використовуваним і важливим інструментом для обробки природної мови в області доступу до інформації. Стеммінг використовується для видалення слів, які додають морфологічні та діакритичні закінчення слів в англійській мові до їх кореневої форми для вилучення кореня слова, так званого стема, на етапі первинної обробки тексту. Іншими словами, це лінгвістичний процес, який просто витягує основну частину, яка може бути близькою до відносного та спорідненого кореня. Класифікація текстів є одним з основних завдань при добуванні відповідної інформації з великого обсягу даних. У даній роботі ми пропонуємо способи поліпшення версії алгоритму Портера з метою обробки і подолання його обмежень, а також економії часу і пам'яті за рахунок зменшення розміру слів. Система використовує вдосконалену техніку виведення Портера для скорочення слів в той час як виконує когнітивні обчислення для виявлення морфологічно пов'язаних слів з корпусу без будь-якого втручання людини або спеціальних мовних знань. Вдосконалений алгоритм Портера порівнюється з вихідним стеммером. Вдосконалений алгоритм Портера має більш високу продуктивність і забезпечує більш точний пошук інформації (ПІ).

Ключові слова: алгоритм стеммінга, обробка природної мови, пошук інформації, ВАСП, алгоритм Портера.

DOI: 10.15587/1729-4061.2021.225346**РОЗРОБКА МЕТОДУ ПОБУДОВИ ЛІНГВІСТИЧНИХ ЕТАЛОНІВ ДЛЯ МУЛЬТИКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ HONEYPOT (с. 14–23)****А. О. Корченко, В. О. Бреславський, С. П. Євсєєв, Н. К. Жумангалієва, А. О. Зварич, С. В. Казмірчук, О. А. Курченко, О. А. Лаптев, О. В. Северінов, С. С. Ткачук**

Один з актуальних напрямків, який розвивається в сфері інформаційної безпеки, пов'язаний з використанням Honeypot (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найбільш ефективних Honeypot і подальша їх класифікація є актуальним завданням. Наведено основні продукти, в яких реалізовані технології віртуальних приманок. Найчастіше вони використовуються для вивчення поведінки, підходів і методів, які використовує неавторизована сторона для несанкціонованого доступу до ресурсів інформаційних систем. Онлайн-пастки можуть імітувати будь-який ресурс, але частіше за все вони виглядають як справжні виробничі сервери і робочі станції. Відомий ряд досить ефективних розробок, які використовуються для вирішення завдань виявлення атак на ресурси інформаційних систем, в основу яких закладено апарат нечітких множин. Вони показали ефективність застосування відповідного математичного апарату, використання якого, наприклад, для формалізації підходу до формування набору еталонних величин, що дозволять удосконалити процес визначення найбільш ефективних Honeypot. З цією метою сформована множина характеристик (процес установки та налаштування, процес використання та підтримки, збір даних, рівень протоколювання, рівень імітації, рівень взаємодії), що визначає властивості онлайн-пасток. Зазначені характеристики стали основою для розробки методу формування еталонів лінгвістичних змінних для подальшого вибору найбільш ефективних Honeypot. Метод базується на формуванні множини Honeypot, підмножин характеристик і значень ідентифікаторів лінгвістичних оцінок характеристик Honeypot, базової і похідної матриці частот, а також на побудові нечітких термів і еталонних нечітких чисел з їх візуалізацією. Це дозволить в подальшому класифікувати і здійснити вибір найбільш ефективних віртуальних приманок.

Ключові слова: класифікація honeypot, віртуальні приманки, нечіткі еталони, метод формування лінгвістичних еталонів.

DOI: 10.15587/1729-4061.2021.225339**РОЗРОБКА АЛГОРИТМУ ЗАХИСТУ ПРИСТРОЇВ КОМУНІКАЦІЇ КОРИСТУВАЧІВ ВІД ВИТОКІВ ДАНИХ (с. 24–34)****О. В. Задерейко, Ю. В. Прокоп, О. Г. Трофименко, Н. І. Логінова, О. Є. Плачинда**

З метою виявлення шляхів збору даних з пристроїв комунікації користувачів було проведено аналіз взаємодії клієнтів DNS з доменним простором імен Інтернет. Встановлено, що DNS трафік пристрою комунікації журналюється DNS серверами провайдера, що саме по собі несе загрозу приватності користувачів. Розроблено та апробовано комплексний алгоритм захисту від збору даних користувачів, який складається з двох модулів. Перший модуль дозволяє перенаправити DNS трафік пристрою комунікації через DNS проксі-сервери з заданим класом анонімності, визначеним на основі запропонованого мультитесту. Для забезпечення безперерійного і сталого з'єднання модуль здійснює автоматичне підключення до DNS проксі-сервера з мінімальним часом відгуку з доступних у сформованому списку. Другий модуль блокує збір даних, який здійснюється розробниками програмного забезпечення, встановленого на пристрої комунікації користувача, та спеціалізованими інтернет-сервісами, які належать ІТ-компаніям. Запропонований алгоритм дозволяє користувачам вибирати бажаний рівень приватності при здійсненні комунікації з інтернет-простором. Це дозволяє знизити ймовірність цифрового профілювання пристроїв комунікації і, як наслідок, позбавити можливості інформаційних маніпуляцій над їх власниками. Проведено комплексний аудит DNS трафіка різних стаціонарних і мобільних пристроїв комунікації. Аналіз DNS трафіка

дозволив ідентифікувати і структурувати DNS запити, які відповідають за збір даних користувачів інтернет-сервісами, що належать IT-компаніям. Виконано блокування ідентифікованих DNS запитів й експериментально підтверджено відсутність втрат працездатності базового і прикладного програмного забезпечення на пристроях комунікації користувача.

Ключові слова: DNS запит, DNS сервер, витоки DNS, DNS трафік, DNS проксі-сервер, збір даних.

DOI: 10.15587/1729-4061.2021.225383

ОПТИМАЛЬНІ ЗНАЧЕННЯ ПАРАМЕТРІВ ПІД-РЕГУЛЯТОРА ДЛЯ ДВИГУНА ПОСТІЙНОГО СТРУМУ НА ОСНОВІ МОДИФІКОВАНОГО МЕТОДУ РОЮ ЧАСТИНОК З АДАПТИВНОЮ ВАГОЮ ІНЕРЦІЇ (с. 35–45)

Mohammed Obaid Mustafa

Суттєвою проблемою в області управління є настройка параметрів ПІД-регулятора. Через його високу нелінійність управління системою двигуна постійного струму є складним і математично повторюваним. Метод рою частинок (МРЧ) є відмінним методом оптимізації і перспективним підходом до вирішення проблеми оптимізації ПІД-регулятора. У даній роботі запропоновано модифікований метод МРЧ з чотирма функціями ваги інерції для знаходження глобальних оптимальних параметрів ПІД-регулятора для управління швидкістю і положенням двигуна постійного струму. Описуються порівняльні дослідження функцій ваги інерції. Для модифікації МРЧ були запропоновані два сценарії, М1-МРЧ і М2-МРЧ, а також класичні алгоритми МРЧ. Для першого сценарію модифікація МРЧ здійснювалася на основі зміни чотирьох функцій ваги інерції, соціального і персонального коефіцієнта прискорення, тоді як у другому сценарії чотири функції ваги інерції були змінені, але соціальний і персональний коефіцієнт прискорення залишався постійним під час реалізації алгоритму. Було проведено порівняння представлених сценаріїв з традиційними ПІД, задовільні результати моделювання показали, що перший сценарій володіє високою швидкістю пошуку, а також дуже ефективною і швидкою реалізацією в порівнянні з другим сценарієм і класичним МРЧ і навіть поліпшеним методом МРЧ. Крім того, запропонований підхід має більш високу швидкість пошуку в порівнянні з класичним МРЧ. Однак було встановлено, що класичний алгоритм МРЧ має передчасний, неточний і локальний процес збіжності при вирішенні складних задач оптимізації. Представлений алгоритм запропонований для збільшення швидкості пошуку вихідного МРЧ.

Ключові слова: налаштування ПІД-регулятора, метод рою частинок, двигун постійного струму, функції ваги інерції.

DOI: 10.15587/1729-4061.2021.225517

СИНТЕЗ СИСТЕМИ УПРАВЛІННЯ СИНХРОНІЗАЦІЄЮ СУДНОВИХ ГЕНЕРАТОРНИХ АГРЕГАТІВ (с. 45–63)

В.В. Будашко, В. А. Шевченко

Статтю присвячено побудові принципів і синтезу системи ефективного управління процесами синхронізації генераторних агрегатів (ГА), що знаходяться у складі розподілених МП-систем управління складними судновими технічними системами і комплексами (СТС і К). Поставлені завдання синхронізації, побудовані моделі процесів, баз даних і визначені конфігурації систем. На основі використання результатних функцій визначені етапи розв'язку завдань управління синхронізацією припасуванням частоти у ієрархічній послідовності. Проведено аналіз функціонування елементів управління СТС і К, запропоновано використання інтегральних критеріїв оптимізації і принципів дуального управління. Показані практичні способи управління синхронізацією ГА. Розв'язано задачу швидкодіючого управління частотою синхронізованих об'єктів на основі принципів припасування. Це дозволило визначити з упередженням часу моменти включення ГА при детермінованій і стохастичній постановці завдання синхронізації. Наведені результати експериментальних досліджень процесів синхронізації ГА і доведена ефективність запропонованого управління ГА. Принципи побудови процедур управління складом ГА методом «жорстких» і «гнучких» порогів дозволили визначити критерії оптимізації та реалізувати закон управління, який задовільнив умові екстремуму, що є показником досяжності поставленої мети і враховує обмеження керуючих впливів. Розроблена система у класі адаптивних систем управління відбулася завдяки відповідній декомпозиції елементів системи поділенням завдання синхронізації на завдання швидкодії і завдання управління у затребуваних умовах. Наведені приклади процесів невдалої синхронізації з використанням стандартних алгоритмів управління синхронізатором і процесів вдалої синхронізації ГА – з використанням запропонованих алгоритмів дуального управління синхронізатором підтвердили достовірність основних отриманих наукових результатів.

Ключові слова: технічна експлуатація, синхронізація, якість, система управління, математичне моделювання.