Russian Technological Journal.
2022;10(6):20–27

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 004.49
https://doi.org/10.32362/2500-316X-2022-10-6-20-27

RESEARCH ARTICLE

Genetic programming support vector machine model for a wireless intrusion detection system

Anshita Dhoot [1, @], Alexey N. Nazarov [2], Ilia M. Voronkov [3]

[1] *Moscow Institute of Physics and Technology, Moscow oblast, Dolgoprudny, 141701 Russia*
[2] *MIREA – Russian Technological University, Moscow, 119454 Russia*
[3] *HSE University, Moscow, 123557 Russia*
[@] *Corresponding author, e-mail: anshita.dhoot.23@gmail.com*

Abstract

Objectives. The rapid penetration of wireless communication technologies into the activities of both humans and Internet of Things (IoT) devices along with their widespread use by information consumers represents an epochal phenomenon. However, this is accompanied by the growing intensity of successful information attacks, involving the use of bot attacks via IoT, which, along with network attacks, has reached a critical level. Under such circumstances, there is an increasing need for new technological approaches to developing intrusion detection systems based on the latest achievements of artificial intelligence. The most important requirement for such a system consists in its operation on various unbalanced sets of attack data, which use different intrusion techniques. The synthesis of such an intrusion detection system is a difficult task due to the lack of universal methods for detecting technologically different attacks; moreover, the consistent application of known methods is unacceptably long. The aim of the present work is to eliminate such a scientific gap.

Methods. Using the achievements of artificial intelligence in the fight against attacks, the authors proposed a method based on a combination of the genetic programming support vector machine (GPSVM) model using an unbalanced CICIDS2017 dataset.

Results. The presented technological intrusion detection system architecture offers the possibility to train a dataset for detecting attacks on CICIDS2017 and extracting detection objects. The architecture provides for the separation of the dataset into verifiable and not verifiable elements, with the latter being added to the training set by feedback. By training the model and improving GPSVM training set, better accuracy is ensured. The operability of the new flowchart of the GPSVM model is demonstrated in terms of the entry of input data and output of data after processing using the training set of the GPSVM model. Numerical analysis based on the results of model experiments on selected quality indicators showed an increase in the accuracy of the results as compared to the known SVM method.

Conclusions. Computer experiments have confirmed the methodological correctness of choosing a combination of the GPSVM model using an unbalanced CICIDS2017 dataset to increase the effectiveness of intrusion detection. A procedure for forming a training dataset based on feedback is proposed. The procedure involving the separation of datasets is shown to create conditions for improving the training of the model. The combination of the GPSVM model with an unbalanced CICIDS2017 dataset to collect a sample increases the accuracy of intrusion detection to provide improved intrusion detection performance as compared to the SVM method.

Keywords: cyber security, cyber intrusion detection, rare category detection, IDS dataset, GPSVM

• **Submitted:** 15.02.2022 • **Revised:** 19.04.2022 • **Accepted:** 12.09.2022

For citation: Dhoot A., Nazarov A.N., Voronkov I.M. Genetic programming support vector machine model for a wireless intrusion detection system. *Russ. Technol. J.* 2022;10(6):20–27. https://doi.org/10.32362/2500-316X-2022-10-6-20-27

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Модель GP SVM для беспроводной системы обнаружения вторжений

А. Дхут [1, @], А.Н. Назаров [2], И.М. Воронков [3]

[1] *Московский физико-технический институт (национальный исследовательский университет), Московская область, г. Долгопрудный, 141701 Россия*
[2] *МИРЭА – Российский технологический университет, Москва, 119454 Россия*
[3] *Национальный исследовательский университет «Высшая школа экономики», Москва, 123557 Россия*
[@] *Автор для переписки, e-mail: anshita.dhoot.23@gmail.com*

Резюме

Цели. Стремительное проникновение технологий беспроводной связи и устройств Интернета вещей (IoT) в деятельность человека и их повсеместное использование потребителями информации является значимым историческим явлением. Этот процесс сопровождается растущей интенсивностью негативных информационных атак, прежде всего, широким распространением бот-атак через IoT, объем которых наряду с сетевыми атаками достигает критического уровня, и снизить его самостоятельно потребителям контента не представляется возможным. В таких обстоятельствах возрастает потребность в синтезе технологически новой, основанной на новейших достижениях искусственного интеллекта, системы обнаружения вторжений. Важнейшим требованием к системе является ее эффективность при работе на полученных разными способами несбалансированных наборах данных атак, использующих разные технологические приемы вторжения. Синтез такой системы обнаружения вторжений является сложной задачей из-за отсутствия универсальных методов обнаружения технологически разных атак, а последовательное применение известных методов является недопустимо долгим. Ликвидация этого научного пробела и является целью настоящей статьи.

Методы. Используя достижения искусственного интеллекта в борьбе с атаками, авторы предложили способ, основанный на комбинации модели машины опорных векторов генетического программирования (GPSVM) с применением несбалансированного набора данных CICIDS2017.

Результаты. Предложена архитектура системы технологического обнаружения вторжений с возможностью целевого обучения набора данных в интересах обнаружения атак на CICIDS2017 и извлечения объектов обнаружения. Архитектурой предусмотрено разделение набора данных на проверяемые и непроверяемые объекты, которые по результатам обратной связи будут добавлены в обучающий набор. Для того чтобы обеспечить лучшую точность результата, происходит обучение модели и совершенствование обучающего набора GPSVM. Показана работоспособность новой блок-схемы модели GPSVM относительно того, как набор данных вводится в качестве входных данных и выдает выходные данные после обработки с помощью обучающего набора модели GPSVM. Численный анализ результатов модельных экспериментов по выбранным показателям качества показал увеличение точности результатов по сравнению с известным методом SVM.

Выводы. Компьютерные эксперименты подтвердили методическую правильность выбора комбинации модели GPSVM с применением несбалансированного набора данных CICIDS2017 для повышения эффективности

обнаружения вторжений. Предложена процедура формирования обучающего набора данных, основанная на обратной связи. Показано, что применение такой процедуры вместе с разделением наборов данных создает условия для совершенствования обучения модели. Комбинация модели GPSVM с несбалансированным набором данных CICIDS2017 для сбора выборки повышает точность обнаружения вторжений и обеспечивает наилучшую производительность обнаружения вторжений по сравнению с методом SVM.

Ключевые слова: кибербезопасность, обнаружение кибератак, обнаружение редких категорий, набор данных IDS, GPSVM

• **Поступила:** 15.02.2022 • **Доработана:** 19.04.2022 • **Принята к опубликованию:** 12.09.2022

Для цитирования: Dhoot A., Nazarov A.N., Voronkov I.M. Genetic programming support vector machine model for a wireless intrusion detection system. *Russ. Technol. J.* 2022;10(6):20–27. https://doi.org/10.32362/2500-316X-2022-10-6-20-27

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

In order to defend a system from malicious behaviors such as attacks and malware, it is necessary to ensure intrusion detection. An intrusion detection system (IDS) represents an essential line of defense to protect complicated networks against increasing activities of intruders. For this reason, improved IDS designs based on wide-ranging and valid datasets for testing and evaluating techniques are proposed [1], along with responses to the challenge of obtaining significant datasets [2].

Some datasets are not shareable because of privacy concerns, while other available datasets do not reflect the latest trends. Moreover, many datasets are anonymized, despite the variety of traffic involving diverse evidence-based attacks. Thus, there are problems concerning a scarcity of definite characteristics, as well as the general inaccessibility of datasets. Hence, a precisely seamless dataset is yet to be comprehended [2–4]. Due to the evolution of malware and consistently changing attack strategies, it is necessary to regularly update standard datasets [2].

Since the year 1999, many frameworks for evaluating the IDS dataset have been proposed [2–9]. As per the latest existing research evaluation of frameworks, namely diversity of attacks, even characteristics, presented protocols, anonymity, wide-ranging interaction, complete capture, comprehensive network configuration, featuring dataset, ample traffic, metadata, heterogeneity, as well as labelling, are critical factors for developing a valid and comprehensive IDS dataset [7, 9].

ATTACK TYPES AND SCENARIOS

The IDS dataset of the Canadian Institute for Cybersecurity (CICIDS2017 dataset[1]), which offers a wide diversity of attacking sources, is intended for intrusion detection purposes, as well as providing generally network security. This dataset identifies six common attack types, which can be executed using required tools and codes [10–13].

- *Brute force attack:* Perhaps the best-known form of attack, used for password cracking as well as discovering hidden pages and available content in web applications. This type of attack is based on trial and error until the intruder succeeds.
- *Denial-of-service* (*DoS*) *Attack*: A kind of attack in which the intruder seeks to make a machine or network resource temporarily unavailable. It accomplishes this by flooding target network/resources/machines with excessive requests to overload the system, preventing some or all authentic requests from being satisfied.
- *Botnet:* An internet-connected device that uses a botnet owner for performing several tasks. This can be used to steal data, provide access for intruders and send spam messages to devices and their connection.
- *Heartbleed Attack:* This is a kind of bug that exists in the OpenSSL cryptography library that is widely used for Transport Layer Security (TLS) protocol implementation, which can be overloaded by sending a heartbeat appeal comprising malformed bulky length field as well as small payload to the susceptible user server to aggravate the target's reaction.
- *DDoS Attacks:* Distributed denial-of-service occurs when there are multiple resources flooded with the large bandwidth or resources of a vulnerable victim that can be targeted easily. In such a situation, an attack can harm a lot of multiple victims that can be compromised resources, for instance botnet; it can be easily targeted to flood system to generate the large traffic network.
- *Information Attack:* Network intrusion from inside usually gets exploited by vulnerable software for instance Adobe Acrobat Reader. After intruding to the software successfully from the backdoor, it

[1] https://www.unb.ca/cic/datasets/ids-2017.html. Accessed November 1, 2021.

conducts discrete attacks on the network of the dupe which is generally known as full-port scan, service inventories by using Nmap, and IP sweep.

- *Web Attack:* A kind of attack that occurs every day to affect individuals, as well as organizations. Structured query language (SQL) injection can be used by an intruder to generate a SQL command string for use to access information held in databases. Cross-site scripting (XSS) is used to inject SQL scripts and brute forcing over HTTP to obtain admin ID-password data.

SAMPLING TECHNIQUES

Several sample techniques are often used in unbalanced class distribution for handling real-world datasets over the network ID and credit-card fraud detection proposed by researchers for handling unbalanced class distribution data to improve classification performance [9]:

- *Over Sampling:* After replicating instances of the minority class, this approach then generates replicates based on minority classes' characteristics that decrease their distinctiveness to reduce the overall class imbalance level.
- *Under Sampling:* Removes the existed instances in the majority for balancing a dataset.
- *Combining Sampling:* Data cleaning method using a combination of sampling techniques to enhance the classification performance of an unbalanced dataset. Includes under- and oversampling, where under sampling is applied prior to oversampling in order to prevent data from being overlapped.

1. PROPOSED WORK

Our contribution: In this paper, we contribute a better result for feature selection using a genetic programming support vector machine (GPSVM) model that covers all the other important criteria to support the system for detecting intrusion attacks. In order to accomplish tests to determine the extracted features which are benign, as well as to analyze dataset for featuring best feature dataset for distinguishing distinct attacks, we used the CICIDS2017 dataset available on the Canadian Institute for Cybersecurity website [14].

This paper expands on earlier methods used as a toolset with which to create tagged datasets that can include data from both host logs and network traffic [15]. In this case, the discussed problem of using unbalanced classes and the approach to batch training of a neural network intrusion classifier with unbalanced classes can be solved by analogy with the results shown in the paper [16].

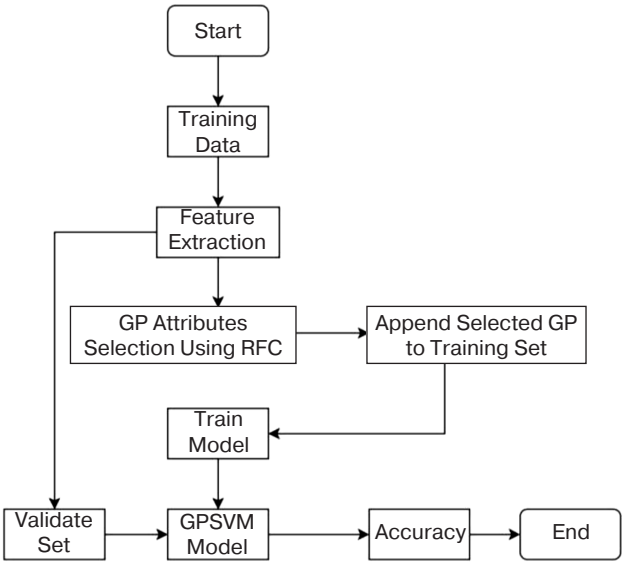

Fig. 1. Flowchart of GPSVM

In our proposed architecture, after carried out training on the CICIDS2017 dataset, features are extracted. For this purpose, datasets are divided into a valid dataset and a dataset that could not be validated, which is sent to genetic programming (GP) attribute selection using request for comments (RFC), after which the selected GP attribute is appended to the training set and sent to the trained model. After that, both datasets go to the GPSVM model to provide better accuracy. Figure 1 shows the flowchart of the GPSVM model as to how the dataset is entered as input to provide an output following its processing via the GPSVM model training set.

2. DATA ANALYSIS

The paper [9] introduced techniques to evaluate random under-sampling (RUS) and synthetic minority over-sampling techniques (SMOTE) and their combination to check the true positive rate of ID results. It shows that RUS gives the superlative performance over the SMOTE that improved results.

While there are a number of available datasets for detecting intrusion attacks, the best dataset as per ID attack is the CICIDS2017, which comprises eight separate files, each containing network activities that have data for five days. After adding eight files to CICIDS2017 dataset, it gives 2830743 instances, 15 classes, and 78 features without any replicated data [9, 14]. However, this dataset is extremely unstable due to the benign class comprising some 80.30% of the dataset. Table 1 shows the CICIDS2017 dataset class distribution with attack labels and the percentage of instances in it.

Below are the three common information that retrieves the evaluation metrics as in this form, precision (P), recall (R), and F-measure (F). Precision (P)

Table 1. CICIDS2017 dataset instances with attack details

No.	Label of attack	Instances	Percentage of total instances
1	Benign attack	2273097	80.3004
2	DoS hulk attack	231073	8.163
3	PortScan attack	158930	5.6144
4	DDoS attack	128027	4.5227
5	DoS Goldeneye attack	10293	0.3636
6	FTP Patator attack	7938	0.2804
7	SSH Patator attack	5897	0.2083
8	DoS Slowloris attack	5796	0.2048
9	DoS Slowhttptest attack	5499	0.1943
10	Bot attack	1966	0.0695
11	Web-Brute force attack	1507	0.0532
12	Web attack XSS	652	0.023
13	Infiltration attack	36	0.0013
14	Web attack-SQL injection attack	21	0.0007
15	Heartbleed attack	11	0.0004
	Total	2830743	100

represents the ratio of accurately classified attacks flow as true positive (*TP*) in the entire classified flows (*TP* + *FP*), where *FP* is false positive:

$$P = \frac{TP}{TP + FP}.$$

Recall (*R*) is also known as sensitivity, which is a ratio of accurately classified attack flows, i.e., *TP*, to the generated flows, i.e., (*TP* + *FN*), where *FN* is false negative:

$$R = \frac{TP}{TP + FN}.$$

F-measure is the harmonic measurement combination of recall and precision in the single measurement:

$$F = \frac{2}{\frac{1}{P} + \frac{1}{R}}.$$

At the time of execution, training, as well as testing process, is calculated to observe the execution. The weighted average of the three evaluations is considered as comprising a result in the form of (*P*, *R*, *F*) that provides the highest accuracy belonging to the renowned algorithms, i.e., *k* nearest neighbor (KNN), iterative dichotomizer 3 (ID3), and random forest (RF) methods.

3. RESULTS

In this paper, we have conducted some tests and compared the support vector machine (SVM) model and GPSVM and received better results with the GPSVM model. Although, SVM gives a good result, GPSVM model gives more accuracy in comparison to the SVM model [17]. Table 2 shows the comparison of the confusion matrix in the SVM and GPSVM models, whereas Table 3 shows model accuracy and cross-validation mean score among the SVM and GPSVM models.

Table 2. Confusion matrix

Models	Confusion matrix
SVM	[[62697 88] [166 47663]]
GPSVM	[[62699 86] [73 47756]]

Table 3. Comparison of SVM and GPSVM models

Models	Model accuracy	Cross-validation mean score
SVM	0.99770726422368	0.9974415541592128
GPSVM	0.998562589334081	0.998499276484312

Figure 2 depicts the model accuracy (1) and cross-validation mean scores (2) to compare the SVM and GPSVM models, supporting the conclusion that the GPSVM model works better than any other current alternative. In order to test both the SVM and GPSVM models, we used the CICIDS2017 dataset for making IDS better to track down intrusion attacks and reduce the attack scenario.

Figure 3 shows important features in the GPSVM model. In our proposed model, the model accuracy enhances the IDS from being vulnerable and gives better output compared to other models.

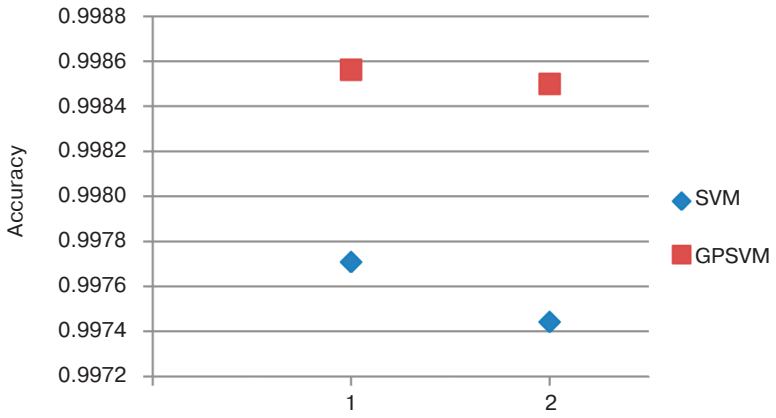

Fig. 2. Comparison of GPSVM and SVM models:
1—model accuracy; 2—cross-validation mean score

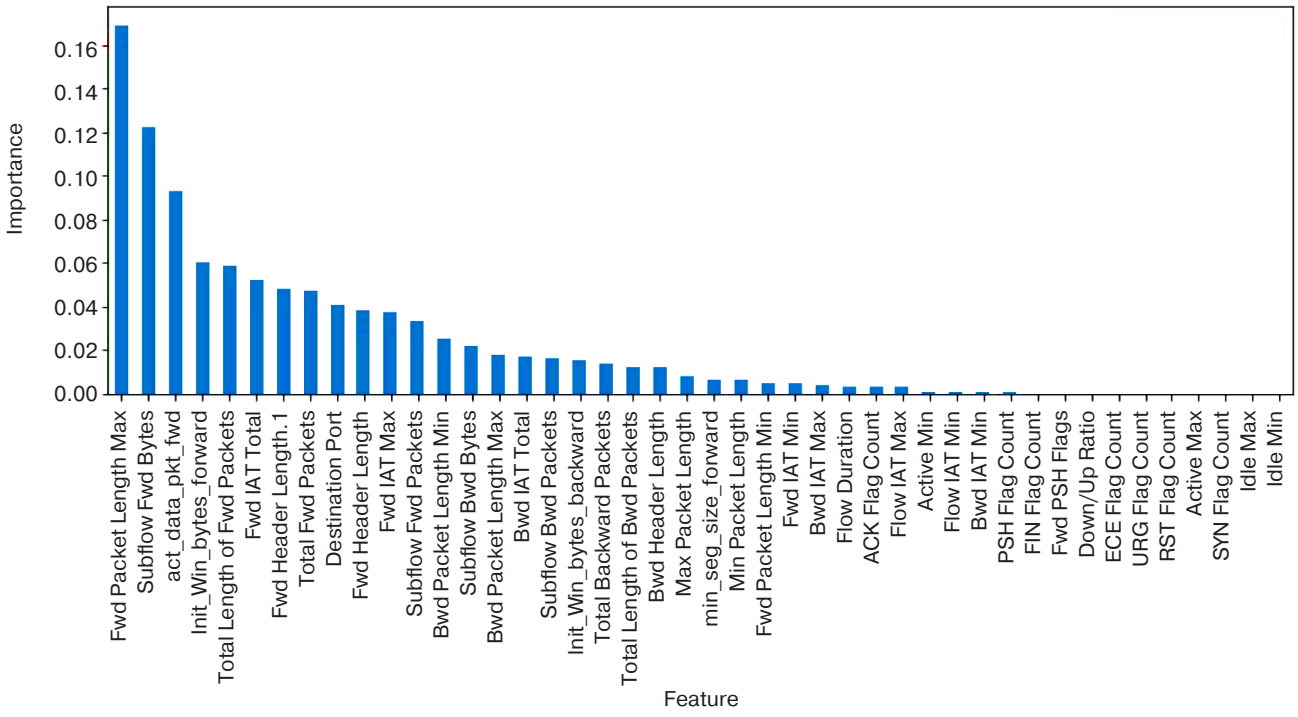

Fig. 3. Important features in the GPSVM model

4. CONCLUSIONS

The presented GPSVM model is concluded to offer an improved approach to tracking intrusion detection that helps to exploit vulnerable systems. This model provides enhanced accuracy for detecting intrusion attacks. In the future, testing this model using a wider variety of resources, along with real-time systems will help to improve the integration of the GPSVM feature extraction technique to develop an improved model version. This will aid IDSs development to improve the reliability of intrusion-detecting machines for various intrusion types. The proposed approach can be used as part of a cloud service for monitoring cyber-attacks using neuro-fuzzy formalism.

ACKNOWLEDGMENTS

The reported was funded by the Russian Foundation for Basic Research, No. 21-57-54002, and Vietnam Academy of Science and Technology, No. QTRU01.14/21-22, 2021.

Authors' contribution

All authors equally contributed to the research work. All authors approved the final text of the manuscript for publication.

Вклад авторов

Все авторы внесли равный вклад в исследование. Все авторы прочитали и согласны с окончательным текстом статьи.

REFERENCES

1. Koch R., Golling M., Rodosek G.D. Towards comparability of intrusion detection systems: New data sets. In: *TERENA Networking Conference* (*TNC*). 2014. V. 7.
2. Nehinbe J.O. A critical evaluation of datasets for investigating IDSs and IPSs researches. In: *2011 IEEE 10th International Conference on Cybernetic Intelligent Systems* (*CIS*). IEEE; 2011. P. 92–97. https://doi.org/10.1109/CIS.2011.6169141
3. Shiravi A., Shiravi H., Tavallaee M., Ghorban A.A. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security.* 2012;31(3):357–374. https://doi.org/10.1016/j.cose.2011.12.012
4. Ghorbani A.A., Lu W., Tavallaee M. Detection approaches. In: *Network Intrusion Detection and Prevention.* Boston, MA: Springer; 2010. P. 27–53. https://doi.org/10.1007/978-0-387-88771-5_2
5. Scott P.D., Wilkins E. Evaluating data mining procedures: techniques for generating artificial data sets. *Inf. Softw. Technol.* 1999;41(9):579–587. https://doi.org/10.1016/S0950-5849(99)00021-X
6. Heidemann J., Papdopoulos C. Uses and challenges for network datasets. In: *2009 Cybersecurity Applications & Technology Conference for Homeland Security.* IEEE; 2009. P. 73–82. https://doi.org/10.1109/CATCH.2009.29
7. Gharib A., Sharafaldin I., Lashkari A.H., Ghorbani A.A. An evaluation framework for intrusion detection dataset. In: *2016 International Conference on Information Science and Security* (*ICISS*). IEEE; 2016. P. 1–6. https://doi.org/10.1109/ICISSEC.2016.7885840
8. Sharafaldin I., Gharib A., Lashkari A.H., Ghorbani A.A. Towards a reliable intrusion detection benchmark dataset. *Software Networking*. 2018;2017(1):177–200. https://doi.org/10.13052/jsn2445-9739.2017.009
9. Ho Y.B., Yap W.S., Khor K.C. The effect of sampling methods on the CICIDS2017 network intrusion data set. In: Kim H., Kim K.J. (Eds.). *IT Convergence and Security*. *Lecture Notes in Electrical Engineering*. Singapore: Springer; 2021. V. 782. P. 33–41. https://doi.org/10.1007/978-981-16-4118-3_4
10. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy* (*ICISSP*). 2018. P. 108–116. https://doi.org/10.5220/0006639801080116
11. Bashir T., Agbata B.C., Ogala E., Obeng-Denteh W. The fuzzy experiment approach for detection and prevention of masquerading attacks in online domain. *East African Sch. J. Eng. Comput. Sci.* 2020;3(10):205–215. https://doi.org/10.36349/easjecs.2020.v03i10.001
12. Fang Y., Zhang C., Huang C., Liu L., Yang Y. Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism. *IEEE Access*. 2019;7:56329–56340. https://doi.org/10.1109/ACCESS.2019.2913705
13. Zhu E., Ju Y., Chen Z., Liu F., Fang X. DTOF-ANN: An artificial neural network masquerading detection model based on decision tree and optimal features. *Appl. Soft Comput.* 2020;95:106505. https://doi.org/10.1016/j.asoc.2020.106505
14. Lashkari A.H., Draper-Gil G., Mamun M.S.I., Ghorbani A.A. Characterization of tor traffic using time-based features. In: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy* (*ICISSP*). 2017, February. P. 253–262. https://doi.org/10.5220/0006105602530262
15. Nazarov A.N., Sychev A.K., Voronkov I.M. The role of datasets when building next generation intrusion detection systems. In: *2019 Wave Electronics and its Application in Information and Telecommunication Systems* (*WECONF*). IEEE; 2019. https://doi.org/10.1109/WECONF.2019.8840124
16. Pantiukhin D., Nazarov A., Voronkov I.M. Intelligent methods for intrusion detection in local area networks. In: Pozin B., Cavalli A.R., Petrenko A. (Eds.). *Actual Problems of System and Software Engineering. Proceedings of the 6th International Conference* (*APSSE 2019*). Moscow; 2019. P. 138–149. URL: http://ceur-ws.org/Vol-2514/paper84.pdf
17. Dhoot A., Zong B., Saeed M.S., Singh K. Security analysis of private intellectual property. In: *2021 International Conference on Engineering Management of Communication and Technology* (*EMCTECH*). IEEE; 2021. https://doi.org/10.1109/EMCTECH53459.2021.9619179

About the authors

Anshita Dhoot, Postgraduate Student, Moscow Institute of Physics and Technology (National Research University) (9, Institutskii per., Moscow oblast, Dolgoprudny, 141701 Russia). E-mail: anshita.dhoot@phystech.edu. https://orcid.org/0000-0002-5024-6194

Alexey N. Nazarov, Dr. Sci. (Eng.), Professor, Department of Corporate Information Systems, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: a.nazarov06@bk.ru. ResearcherID G-3154-2013, Scopus Author ID 7201780424, RSCI SPIN-code 6032-5302, https://orcid.org/0000-0002-0497-0296

Ilia M. Voronkov, Visiting Lecturer, HSE University (11, Pokrovskii bul., Moscow, 109028 Russia); Deputy Head, Center for Neural Network Technologies, International Center for Informatics and Electronics (19, Presnenskii val, Moscow, 123557 Russia). E-mail: ivoronkov@hse.ru. ResearcherID L-6207-2016, Scopus Author ID 24802429000, RSCI SPIN-code 3869-9670, https://orcid.org/0000-0002-1552-5083

Об авторах

Дхут Аншита, аспирант, ФГАОУ ВО «Московский физико-технический институт (национальный исследовательский университет)» (141701, Московская область, г. Долгопрудный, Институтский переулок, д. 9). E-mail: anshita.dhoot@phystech.edu. https://orcid.org/0000-0002-5024-6194

Назаров Алексей Николаевич, д.т.н., профессор, профессор кафедры корпоративных информационных систем Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: a.nazarov06@bk.ru. ResearcherID G-3154-2013, Scopus Author ID 7201780424, SPIN-код РИНЦ 6032-5302, https://orcid.org/0000-0002-0497-0296

Воронков Илья Михайлович, приглашенный преподаватель, ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики» (109028, Россия, Москва, Покровский бульвар, д. 11); заместитель начальника, Центр нейросетевых технологий, Международный центр по информатике и электронике (123557, Россия, Москва, ул. Пресненский Вал, д. 19). E-mail: ivoronkov@hse.ru. ResearcherID L-6207-2016, Scopus Author ID 24802429000, SPIN-код РИНЦ 3869-9670, https://orcid.org/0000-0002-1552-5083

The text was submitted by the authors in English
Edited for English language and spelling by Thomas A. Beavitt