УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2022 Том 22 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2022 Vol. 22 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2022 Том 22 Номер 2

doi: 10.17586/2226-1494-2022-22-2-317-323

A novel framework for the prevention of black-hole in wireless sensors using hybrid convolution network

Jayaraman Kolangiappan[1]✉, Angamuthu Senthil Kumar[2]

[1] Periyar University, Salem, 636011, India
[2] Arignar Anna Government Arts College, Namakkal, 637002, India

[1] jkakshiya@gmail.com✉, https://orcid.org/0000-0001-5093-5822
[2] senthilkumarmca76@gmail.com, https://orcid.org/0000-0001-5131-7428

Abstract

Problems of Wireless Sensor Networks (WSN) are associated with a significant increase in the number of devices on these networks. In this regard, the requirements for the protection and the security of WSN from external influences are increasing significantly. WSN security problems are solved by solving the problem of optimal path routing, energy conservation, and so on. This paper proposes a hybrid model of an efficient packet routing and delivery system to prevent Black-hole attacks. This type of attack is considered the most common on the network due to its unique characteristics. To detect such attacks, a deep learning model using a Convolutional Neural Network (CNN) is proposed. The learning algorithm must be reliable and trustworthy so that attack analysis can be considered at different levels to study the intelligent behavior of network attacks. The paper considers the problem of finding the optimal shortest path using Deep Q-Learning and convolutional neural networks to perform efficient routing and delivery of packets in a safer way. As a result of simulation, the achieved accuracy reached 98.57 %.

Keywords

convolutional neural network, CNN, Deep Q-Learning, wireless sensor network, WSN, routing, trustworthy

For citation: Kolangiappan J., Senthil Kumar A. A novel framework for the prevention of black-hole in wireless sensors using hybrid convolution network. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 2, pp. 317–323. doi: 10.17586/2226-1494-2022-22-2-317-323

УДК 004.89

Новая структура маршрутизации для предотвращения черных дыр в беспроводных датчиках с использованием гибридной сверточной сети

Джаяраман Колангиаппан[1]✉, Ангамуту Сентил Кумар[2]

[1] Университет Перияр, Салем, 636011, Индия
[2] Государственный художественный колледж Ариньяра Анны, Намаккал, 637002, Индия

[1] jkakshiya@gmail.com✉, https://orcid.org/0000-0001-5093-5822
[2] senthilkumarmca76@gmail.com, https://orcid.org/0000-0001-5131-7428

Аннотация

С увеличением количества устройств в беспроводных сенсорных сетях (WSN) появились дополнительные проблемы. В связи с этим возрастают требования к защите таких сетей от внешних воздействий. Проблемы безопасности WSN определяются путем решения задачи оптимальной маршрутизации пути, энергосбережения и др. Предложена гибридная модель эффективной системы маршрутизации и доставки пакетов для предотвращения атак черных дыр. Такой тип атаки считается наиболее распространенным в сети благодаря своим уникальным характеристикам. Для их обнаружения предложена модель глубокого обучения с использованием сверточной нейронной сети (CNN). Алгоритм обучения должен быть надежным и заслуживающим доверия, чтобы анализ атак можно было рассматривать на разных уровнях для изучения их интеллектуального поведения. Рассмотрена задача поиска оптимального кратчайшего пути с использованием Deep Q-Learning и CNN для выполнения эффективной маршрутизации и доставки пакетов более безопасным способом. В результате моделирования достигнута точность 98,57 %.

Ключевые слова
сверточная нейронная сеть, CNN, Deep Q-Learning, беспроводная сенсорная сеть, WSN, маршрутизация, доверие

Ссылка для цитирования: Колангиаппан Дж., Сентил Кумар А. Новая структура маршрутизации для предотвращения черных дыр в беспроводных датчиках с использованием гибридной сверточной сети // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 2. С. 317–323 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-2-317-323

Introduction

Wireless Sensor network comprises a wide range of sensors that are used to observe the surrounding environment, and they send the observed aggregated data to the requested recipient via internet. All the sensor nodes are communicated through Base Station (BS). Some of the components of Wireless Sensor Networks (WSN) are sensor, radios, Wireless Local Area Network adaptors, and evaluation software. Fig. 1 shows the architecture of WSN. There are many critical applications emerged in different fields such as military, hospital area, agriculture, and so on. The devices in the network are growing exponentially and it is predicted that the devices in WSN will be increased to 500 billion by 2025. Since the devices are increasing tremendously, this fast-growing network exhibits many security challenges that need to be addressed to save the WSN from many attacks such as routing attacks. The proposed work considers Black-hole attack as the most catastrophic attack among many routing ones because of its unique nature in blocking the service of the network.

There are many existing solutions for the detection and prevention of Black-hole assaults in WSN. However, routing attacks are still a challenging issue since the route of the network is the target for the attackers to perform malicious activities such as stealing confidential information of the user. Route discovery and maintenance are the two important methods used in routing process. As part of a discovery process, sender will initiate RREQ packet over the network. Receiver will reply to the sender with the path information over RREP packet. Since these messages are broadcasting in the network, there are many RREPs possible for the sender, and the sender will select only the optimal path. After route establishment, it comes route maintenance where data packets are sent over the network between sender and receiver. During route maintenance phase, all the nodes are frequently communicated to inform their reachability status so that any node can be retained in the network. If no information received from a particular node with in any particular time period, say 1s, then that node will be removed from the network with the understanding that the node is disconnected from the network. Generally, attack can be classified as active attack and passive attack. Former will put some effort to harm the network and the latter will just observe the confidential exchanges of information between the nodes without putting any effort. The primary goal of this research is to find an efficient detection mechanism to detect and prevent Black-hole attack inside the network. Black-hole attack is one of DoS attack which drops the packet selectively instead of forwarding it to the recipient. The performance measurement for the evaluation of the proposed work is done in terms of the shortest route and packet delivery rate with the help of Deep Q-learning and Convolutional Neural Network (CNN).

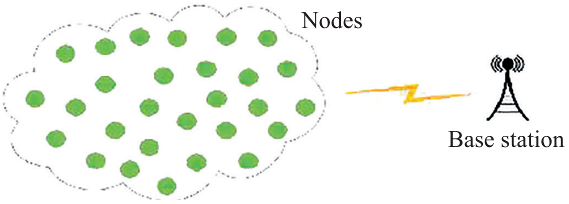

Fig. 1. WSN architecture

Literature Review

Authors in [1] have illustrated that perpetually complex plans of CNN have a new change in Outlook, and the electron diffraction local area has profited from availability of enormous informational collections availability of enormous informational collections also. By a decrease in precision and affectability, the regularly joined CNN, in any case this shift from ordinary highlights design to examine undeniable level provision that is separated from CNN. Especially CNN based gem direction ordering utilizing electron backscatter diffraction is touchy to commotion, lessening the general exactness. With a prepared CNN, another crossover ordering approach has been created to incorporate word reference ordering (DI) with an accomplished phenomenal speed and heartiness against commotion all the while. This work focused only on basic features. The work can be suitable for a small network, they cannot cop up with the large-scale network environment

In [2], the authors proposed a detection framework to detect attacks on health care based WSN. The work introduces a hybrid deep learning using CNN for attack detection. The authors utilized deep learning CNN techniques to detect Black-hole attacks. Numerous scientists have introduced distinctive cutting-edge frameworks dependent on profound learning and AI draws near to defeat this issue. The proposed technique can be applied to health care applications of WSN. The algorithm introduced in the paper can improve the detection accuracy of network attacks comparing the previous existing model. However, it exhibits huge computational cost that degrades the overall performance of the network.

Authors in [3] have proposed the development of Hybrid System (HS) composed of a CNN and a Support Vector Machine (SVM), In order to build a non-destructive tool for the recognition and classification of bread baking stages, based exclusively on the color changes of the bread crust, the present work aims. The HS374 images of the bread crust were used for training, validation and using of distributed over seven baking periods. Without human intervention, overcoming even models based solely on CNN showed that the HSCNN-SVM was able to correctly recognize and classify the baking stages. In favoring its use in mobile or embedded systems, the HSCNN-SVM maintained the ability to extract color map characteristics present in CNN. Even though the work performed well with different features, they cannot cope up with multi variant features to exactly recognize the attack pattern.

Authors in [4] have proposed a new routing algorithm — Opportunistic Routing Protocol (IOP) — for efficient routing in WSN. The algorithm uses NB classification technique to select relay nodes in the network. Authors claim that the proposed technique achieves higher reliability and energy efficiency during the communication. However, it is not clear if the data transmission is secured while perform routing. The current techniques do not give legitimate update results and takes additional time. The proposed Convolutional Neural Organization (CNN) calculation is given with legitimate update results and it gives a brief time frame for consistently updating the strategy. To conquer this issue, numerous scientists have introduced distinctive cutting-edge frameworks dependent on Profound Learning and AI draws near.

Authors in [5] have developed a security framework for WSN, which uses deep learning model using CNN to improve the detection accuracy of DoS (Distributed Denial of Service) attacks. The proposed work can effectively prevent Black-hole attack from the network. However, the work focused only on MAC layer and application layer since these layers are main target for many attacks.

Authors in [6] have proposed a trusted IDS framework for routing attacks. The work uses CNN, RNN (Recurrent Neural Network), and DNN (Deep Neural Network) for the prevention of DoS attack inside the network. The authors use KDD dataset for the result comparison with the regression technique. The work achieves 79 % of detection accuracy when compared to the existing schemes used in the algorithm. Even though the accuracy had improved in the work, most of the important attacks in DoS are not well addressed.

Implementation

Black-hole attack scenario is shown in Fig. 2. In a Black-hole assault, a vindictive hub draws in the information packets by announce a dishonestly, new way to arrive at objective. Be that as it may, it assimilates the information packets and not forward bundles to objective. In helpful Black-hole assault malignant hubs cooperate in a group [7–10]. In a Black-hole assault, a malignant hub draws in the information bundles by pronounce an erroneously, new way to arrive at objective. However, it retains the information packets and not forward bundles to objective. In helpful Black-hole assault, noxious hubs cooperate in a group. Where S is a source hub and D is an objective hub, Nodes 1,2,3,4 and 5 are proceeds as the middle hubs and 4(B1) and 5(B2) Nodes are go about as agreeable Black-hole hubs. At the point when source hub needs to send an information bundle to target, it sends RREQ message to all neighbor hubs. Here the malevolent hubs additionally are the part of the organization and they get the RREQ message. Then, at that point malevolent hubs promptly send the RREP message that range at objective through B1. When source hub gets the RREP, it begins the information bundles to ship off B1 continuously. B1 drops the information packets, and rather sends it to target. Along these lines the information bundle is loosed and never reaches the target.

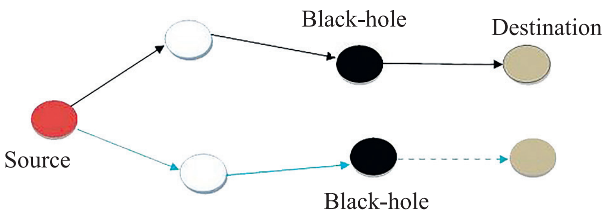

Fig. 2. Black-hole attack

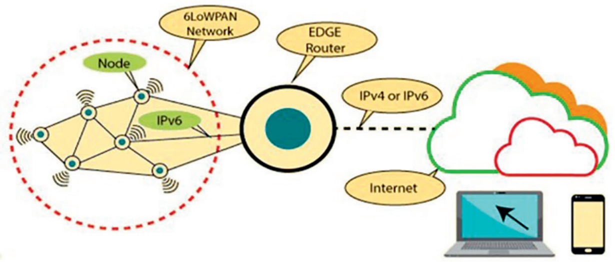

Fig. 3. Network Layer processing

Eventually, Black-hole attack occurs on path of selection and its message distribution to the original administrator nodes. Even though, many researchers are contributing N number of algorithms for shortest path, trustworthy node selection and security issues [11–12]. We implemented hybrid mechanism for route selection and message transmission. Convolution neural network is the contemporary powerful algorithm for digital, text and images training aspects. Before we start our framework, we identified two parameters such as traffic analysis and trustworthy route. In our hybrid model, path has been trained as well as packets are also trained in ML.

Fig. 3 depicts the processing techniques of network layer. Black-hole attacks are playing critical role in this layer for harming the WSN functions. Hence, we established the path using CNN training set. For instance, in WSN 50 nodes are available (Node1 to Node 50); possible trustworthy path will be trained and stored in CNN. Secondarily, both destination and arrival nodes packets will be identified and trained by CNN.

Architecture

We propose a hybrid CNN for obtaining the good performance over the network; it is shown in Fig. 4. In this scenario, we fully utilized features of CNN Layers.

Numerous remote sensor networks require an arrangement of the approaching information as a way for space researchers to better comprehend the gathered information, or with the motivation behind performing

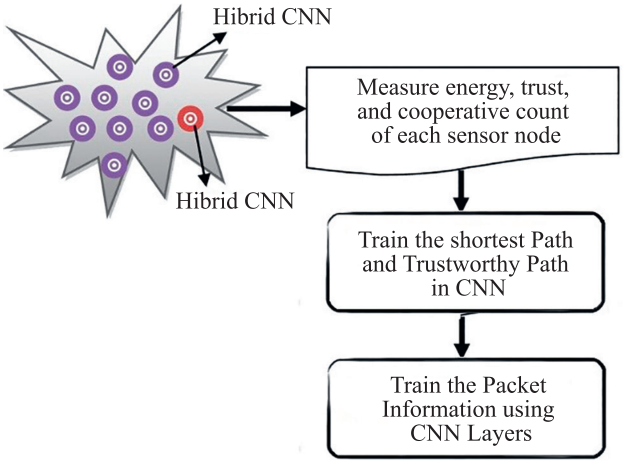
Hibrid CNN
Measure energy, trust, and cooperative count of each sensor node
Hibrid CNN
Train the shortest Path and Trustworthy Path in CNN
Train the Packet Information using CNN Layers

Fig. 4. Proposed architecture

various sorts of incitation in the environment what's more, this should be possible with the assistance of a CNN [13].

Shortest Path finding

Our foremost problem in WSN is finding the shortest path in a heterogeneous network; and it should be trustworthy. We proposed Deep Q-learning methods for finding the shortest path. Q-learning is a without model support learning calculation. The objective of Q-learning is to gain proficiency with a strategy, which mentions to a specialist which move to make under certain conditions. It doesn't need a model of the climate, and it can deal with issues with stochastic advances and rewards, without requiring variations. Q-learning is possessed with the objective function where loss function in a transaction is s, a, r, s'. To begin with, the Q-network forward pass is performed utilizing the state as a contribution to acquire activity esteem as incentive for all activities. In the wake of getting the climate return esteem $<r, s'>$ for the activity a, the activity esteem is an incentive for all activity, and a' is acquired again utilizing the state s' as in equation:

$$L = \frac{1}{2}[\gamma + \max_{a'} Q(s', a') - Q(s, a)]^2.$$

Then, at that point, we get all the data to get the misfortune work, which refreshes the weight boundary, so the Q-esteem refreshes for the chose activity merges; that is, as close as conceivable to the objective worth and the forecast esteem.

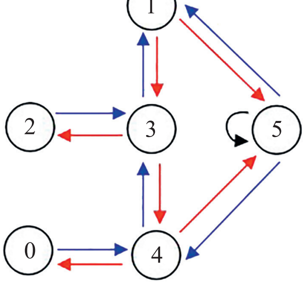

Fig. 5. Deep Q-learning

Fig. 5 shows a maze through which the agent should go and find its way up to the final stage (stage 5). Basically, the idea is to train an algorithm to find the optimal path, given an initial condition (often random), in order to maximize a certain outcome. In this simple example, as you can see from the picture shown in the article, the possible choices are all known and the outcome of each choice is deterministic. A best path exists and can be found easily regardless of the initial condition.

The optimal sequence path is clearly 2 – 3 – 1 – 5.

Q values can be calculated as follows:

$$Q(s, a) \leq (1 - a)Q(s, a) + \alpha(R(s, a) + \gamma \max Q(s', a')),$$

where $Q(s, a)$ is the Q value of an action a from state s to s'; α is the learning rate; $R(s, a)$ is the reward of doing action a from state s to s'; γ is the discount factor; $\max Q(s', a')$ is the max Q value among all possible actions in the next state s.

Packet Delivery using CNN

There are many deep learning models that are categorized in to supervised and unsupervised learning for learning various patterns. CNN and ResNet are used in the work for classification and extraction. We consider only packet data to create deep learning datasets. The packet data is treated as image data. NSL-KDD data that comprises of normal data and malicious data are used in the study for training the proposed detection mechanism. The performance evaluation of the dataset and the proposed detection scheme is done using confusion matrix as shown in Table. We evaluated the work as 10 class classification for malware feature, such as Normal, Buffer overflow, Load module, Perl, Neptune, Smurf, Guess_pwd, Pod, Multihop and Spy. For instance, the value 12 in normal class indicates how correctly we classified 12 test samples of normal pattern. Value of TP, FP, TN, and FN indicates the training positive and negative values of attacks pattern.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TNR} + \text{FNR} + \text{TPR} + \text{FPR}} \cdot 100, \quad (1)$$

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \cdot 100, \quad (2)$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \cdot 100. \quad (3)$$

We took on four ordinarily utilized boundaries for assessing interruption recognition frameworks: Accuracy, True Positive Rate (TPR), False Positive Rate (FPR), and F1-score as shown in equation (1), (2), (3). Accuracy addresses the general presentation of the model, TPR addresses the proportion of the genuine positive example in the current positive example to every certain example, and FPR addresses the proportion of the genuine negative example wrongly allocated to the positive example type to the all-out number of every single negative example. Review addresses the quantity of True Positives partitioned by the quantity of True Positives and the quantity of False Negatives. Exactness addresses the quantity of

Table. CNN Evaluation table

Classes	Normal	Buffer overflow	Load module	Perl	Neptune	Smurf	Guess_pwd	Pod	Multihop	Spy
Normal	12	0	0	0	0	0	0	0 FP	0	0
Buffer overflow	0	10	0	0	0	0	0	0 FP	2	0
Load module	0	0	10	0	0	0	8	0 FP	0	0
Perl	0	0	0	19 TN	0	0	0	0 FP	0TN	0
Neptune	0	0	0	0	19 TN	0	0	0 FP	0	0
Smurf	0	2	3	0	0	15	0	0 FP	0	0
Guess_pwd	0	0	0	0	0	0	16	0 FP	0	0
Pod	1	0FN	0FN	0FN	0FN	2	3	15 TP	0FN	FN
Multihop	0 (ACTU)	0	1	1	0	0	1	FP	13 TN	0
Spy	1	1	0	3 TN	0	0	0	FP (PRED)	0	7

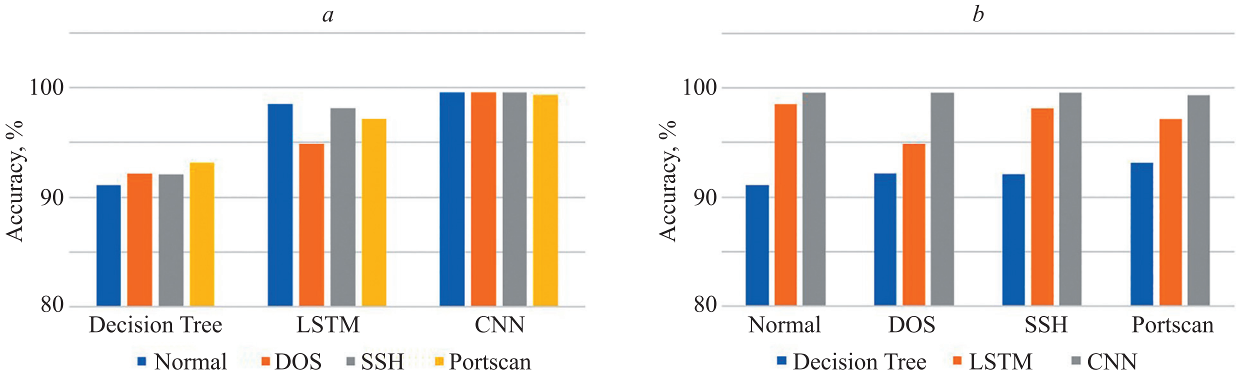

Fig. 6. Comparison with different Learning Algorithm (*a*), Performance Chart (*b*)

positive forecasts separated by the all-out number of positive class esteems anticipated. F1-score is a score of a classifier's exactness and is characterized as the weighted symphonious mean of the Precision and Recall proportions of the classifier.

Result and Discussion

As the first step of the work, optimum path using Q-learning is obtained to find the efficient shortest route among all shortest routes. Even though, this step and Dijikstra's algorithms are efficient in finding shortest route, the drawback of these two algorithms are that they cannot cope up with larger graphs and the algorithm will be very slow while dealing with such graphs [14–16]. The performance evaluation for finding the shortest path using deep Q-learning models is compared with A*, and Dijkstra's algorithms. Even though, these two traditional algorithms are robust in finding shortest routes, they are very slow on large graphs, and more memories are required to store the distances. In this work, we learned many complex graphs using proposed Deep Q (D-Q) learning models.

At the second step, the CNN algorithms are simulated in network scenario for packet delivery analysis of the proposed work. Decision tree, LSTM, and CNN are used for learning different traffic and accuracy of these algorithm under attack condition and without attack condition are shown in Fig. 6.

Conclusion

In contemporary digital world all kinds of human handling things are atomized with Wireless Sensor Networks. Even though, WSN is an ancient technology, but some problems always occur while the transmission, such as shortest Path routing problem, malicious node detection and Black-hole attacks, Gray-hole attacks are the critical concern. We addressed hybrid solution for improving WSN against Black-hole attack. The work performs efficient shortest route with trustworthy nodes and it performs network traffic analysis to find the malicious traffic in the network to mitigate Black-hole attacks. Deep Q-learning was implemented for shortest path, and history has been inputted to CNN for extracting the features of packets in a transmission. Besides, we utilized all the CNN layers in the simulation part. Comparatively, CNN provides high accuracy in the data transmission over DT and LSTM.

References

1. Ding Z., Zhu C., De Graef M. Determining crystallographic orientation via hybrid convolutional neural network. *Materials Characterization*, 2021, vol. 178, pp. 111213. https://doi.org/10.1016/j.matchar.2021.111213
2. Subasini C.A., Karuppiah S.P., Sheeba Adlin, Padmakala S. Developing an attack detection framework for wireless sensor network-based healthcare applications using hybrid convolutional neural network. *Transactions on Emerging Telecommunications Technologies*, 2021, vol. 32, no. 11, pp. e4336. https://doi.org/10.1002/ett.4336
3. da Silva Cotrim W., Felix L.B., Minim V.P., Campos R.C., Minim L.A. Development of a hybrid system based on convolutional neural networks and support vector machines for recognition and tracking color changes in food during thermal processing. *Chemical Engineering Science*, 2021, vol. 240, pp. 116679. https://doi.org/10.1016/j.ces.2021.116679
4. Bangotra D.K., Singh Y., Selwal A., Kumar N., Singh P.K., Hong W-C. An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. *Sensors*, 2020, vol. 20, no. 14, pp. 3887. https://doi.org/10.3390/s20143887
5. Pankaj R. Chandre, Dr. Parikshit N. Mahalle, Dr. Gitanjali R. Shinde. Intrusion prevention framework for WSN using Deep CNN. *Turkish Journal of Computer and Mathematics Education*, 2021, vol. 12, no. 6, pp. 3567–3572.
6. Pasyar P., Mahmoudi T., Kouzehkanan S.Z., Ahmadian A., Arabalibeik H., Soltanian N., Radmard A.R. Hybrid classification of diffuse liver diseases in ultrasound images using deep convolutional neural networks. *Informatics in Medicine Unlocked*, 2021, vol. 22, pp. 100496. https://doi.org/10.1016/j.imu.2020.100496
7. Gulla K.K., Viswanath P., Veluru S.B., Kumar R.R. Machine learning based intrusion detection techniques. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019, pp. 873–888. https://doi.org/10.1007/978-3-030-22277-2_35
8. Jo W., Kim S., Lee C., Shon T. Packet preprocessing in CNN-based network intrusion detection system. *Electronics*, 2020, vol. 9, no. 7, pp. 1151. https://doi.org/10.3390/electronics9071151
9. Yi P., Zhu T., Zhang Q., Wu Y., Li J. A denial of service attack in advanced metering infrastructure network. *Proc. 1st IEEE International Conference on Communications (ICC)*, 2014, pp. 1029–1034. https://doi.org/10.1109/ICC.2014.6883456
10. Wang G., Ren Y., Dou K., Li J. IDTCP: an effective approach to mitigating the TCP incast problem in data center networks. *Information Systems Frontiers*, 2014, vol. 16, no. 1, pp. 35–44. https://doi.org/10.1007/s10796-013-9463-4
11. Wang G., Ren Y., Li J. An effective approach to alleviating the challenges of transmission control protocol. *IET Communications*, 2014, vol. 8, no. 6, pp. 860–869. https://doi.org/10.1049/iet-com.2012.0154
12. Al-Mandhari W., Gyoda K., Nakajima N. Performance evaluation of active route time-out parameter in ad-hoc on demand distance vector (AODV). *Proc. of the 6th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical*, 2008, pp. 47–51.
13. McHugh J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. *ACM Transactions on Information and System Security*, 2000, vol. 3, no. 4, pp. 262–294. https://doi.org/10.1145/382912.382923
14. Draper-Gil G., Lashkari A.H., Mamun M.S.I., Ghorbani A.A. Characterization of encrypted and VPN traffic using time-related features. *Proc. of the 2nd International Conference on Information Systems Security and Privacy (ICISSP)*, 2016, pp. 407–414. https://doi.org/10.5220/0005740704070414
15. Hinton G.E., Srivastava N., Krizhevsky A., Sutskever I., Salakhutdinov R.R. Improving neural networks by preventing co-adaptation of feature detectors. *arXiv*, 2012, arXiv:1207.0580.
16. Wang S., Minku L.L., Yao X. A systematic study of online class imbalance learning with concept drift. *IEEE Transactions on Neural Networks and Learning Systems*, 2018, vol. 29, no. 10, pp. 4802–4821. https://doi.org/10.1109/TNNLS.2017.2771290

Литература

1. Ding Z., Zhu C., De Graef M. Determining crystallographic orientation via hybrid convolutional neural network // Materials Characterization. 2021. V. 178. P. 111213. https://doi.org/10.1016/j.matchar.2021.111213
2. Subasini C.A., Karuppiah S.P., Sheeba Adlin, Padmakala S. Developing an attack detection framework for wireless sensor network-based healthcare applications using hybrid convolutional neural network // Transactions on Emerging Telecommunications Technologies. 2021. V. 32. N 11. P. e4336. https://doi.org/10.1002/ett.4336
3. da Silva Cotrim W., Felix L.B., Minim V.P., Campos R.C., Minim L.A. Development of a hybrid system based on convolutional neural networks and support vector machines for recognition and tracking color changes in food during thermal processing // Chemical Engineering Science. 2021. V. 240. P. 116679. https://doi.org/10.1016/j.ces.2021.116679
4. Bangotra D.K., Singh Y., Selwal A., Kumar N., Singh P.K., Hong W-C. An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare // Sensors. 2020. V. 20. N 14. P. 3887. https://doi.org/10.3390/s20143887
5. Pankaj R. Chandre, Dr. Parikshit N. Mahalle, Dr. Gitanjali R. Shinde. Intrusion prevention framework for WSN using Deep CNN // Turkish Journal of Computer and Mathematics Education. 2021. V. 12. N 6. P. 3567–3572.
6. Pasyar P., Mahmoudi T., Kouzehkanan S.Z., Ahmadian A., Arabalibeik H., Soltanian N., Radmard A.R. Hybrid classification of diffuse liver diseases in ultrasound images using deep convolutional neural networks // Informatics in Medicine Unlocked. 2021. V. 22. P. 100496. https://doi.org/10.1016/j.imu.2020.100496
7. Gulla K.K., Viswanath P., Veluru S.B., Kumar R.R. Machine learning based intrusion detection techniques // Handbook of Computer Networks and Cyber Security: Principles and Paradigms. 2019. P. 873–888. https://doi.org/10.1007/978-3-030-22277-2_35
8. Jo W., Kim S., Lee C., Shon T. Packet preprocessing in CNN-based network intrusion detection system // Electronics. 2020. V. 9. N 7. P. 1151. https://doi.org/10.3390/electronics9071151
9. Yi P., Zhu T., Zhang Q., Wu Y., Li J. A denial of service attack in advanced metering infrastructure network // Proc. of the 1st IEEE International Conference on Communications (ICC). 2014. P. 1029–1034. https://doi.org/10.1109/ICC.2014.6883456
10. Wang G., Ren Y., Dou K., Li J. IDTCP: an effective approach to mitigating the TCP incast problem in data center networks // Information Systems Frontiers. 2014. V. 16. N 1. P. 35–44. https://doi.org/10.1007/s10796-013-9463-4
11. Wang G., Ren Y., Li J. An effective approach to alleviating the challenges of transmission control protocol // IET Communications. 2014. V. 8. N 6. P. 860–869. https://doi.org/10.1049/iet-com.2012.0154
12. Al-Mandhari W., Gyoda K., Nakajima N. Performance evaluation of active route time-out parameter in ad-hoc on demand distance vector (AODV) // Proc. of the 6th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical. 2008. P. 47–51.
13. McHugh J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory // ACM Transactions on Information and System Security. 2000. V. 3. N 4. P. 262–294. https://doi.org/10.1145/382912.382923
14. Draper-Gil G., Lashkari A.H., Mamun M.S.I., Ghorbani A.A. Characterization of encrypted and VPN traffic using time-related features // Proc. of the 2nd International Conference on Information Systems Security and Privacy (ICISSP). 2016. P. 407–414. https://doi.org/10.5220/0005740704070414
15. Hinton G.E., Srivastava N., Krizhevsky A., Sutskever I., Salakhutdinov R.R. Improving neural networks by preventing co-adaptation of feature detectors // arXiv. 2012. arXiv:1207.0580.
16. Wang S., Minku L.L., Yao X. A systematic study of online class imbalance learning with concept drift // IEEE Transactions on Neural Networks and Learning Systems. 2018. V. 29. N 10. P. 4802–4821. https://doi.org/10.1109/TNNLS.2017.2771290

Authors

Jayaraman Kolangiappan — PhD, Research Scholar, Periyar University, Salem, 636011, India, https://orcid.org/0000-0001-5093-5822, jkakshiya@gmail.com

Angamuthu Senthil Kumar — PhD, Assistant Professor, Arignar Anna Government Arts College, Nxamakkal, 637002, India, https://orcid.org/0000-0001-5131-7428, senthilkumarmca76@gmail.com

Received 11.11.2021
Approved after reviewing 14.02.2022
Accepted 17.03.2022

Авторы

Колангиаппан Джаяраман — PhD, исследователь, Университет Перияр, Салем, 636011, Индия, https://orcid.org/0000-0001-5093-5822, jkakshiya@gmail.com

Сентил Кумар Ангамуту — PhD, доцент, Государственный художественный колледж Ариньяра Анны, Намаккал, 637002, Индия, https://orcid.org/0000-0001-5131-7428, senthilkumarmca76@gmail.com

Статья поступила в редакцию 11.11.2021
Одобрена после рецензирования 14.02.2022
Принята к печати 17.03.2022