Journal of Engineering Science and Technology
Vol. 17, No. 5 (2022) 3555 - 3569

5G NETWORK ACCESS SECURITY MODEL THROUGH DEEP NEURAL NETWORKS CLUSTERING

SEBASTIAN CAMILO VANEGAS AYALA[1,*], OCTAVIO JOSÉ SALCEDO PARRA[1,2], BRAYAN LEONARDO SIERRA FORERO[1]

[1]Universidad Distrital Francisco José de Caldas, Faculty of Engineering, Intelligent Internet Research Group, Bogotá D.C., Colombia
[2]Universidad Nacional de Colombia, Department of Systems and Industrial Engineering, Faculty of Engineering, Bogotá D.C., Colombia
*Corresponding Author: scvanegasa@correo.udistrital.edu.co

Abstract

Considering that a problem in the security of access to 5G networks is DOS attacks due to its orientation to IoT, an alternative security model is proposed that provides a solution to this problem and that requires little information from users, and is easy to use, train, configure, with little processing and high portability. This research proposes a security model for 5G Networks wireless access (5GDoSec) intended to detect possible intruders and malicious users through the use of Deep Neural Networks and the machine learning technique; this is based on the access data collected from a delimited entrance point that groups, identify and classify the authenticated users in the network to detect, based on the access numbers and the active time, the ones that could represent a threat. The 5GDoSec model follows an evolutive character proved to be reliable when classifying hazardous users showing better performance in its validation by DaviesBouldin than other techniques such as Kmeans and Linkage.

Keywords: 5G, Artificial intelligence, Clustering, Machine learning, Security.

1. Introduction

The traditional networks' approach cannot keep up with the advances in terms of the operation, optimization, and management of the next based on services network generation; that requires a unique infrastructure supporting a variety of flexible and efficient services such as improved mobile broadband and reliable massive communication with low latency rates [1, 2]. Therefore, considering the inevitable transition to automated and non-direct control, it is necessary to implement a novel paradigm that is to include proactive, self-conscious, and adaptive-predictive networks within the Big Data analysis framework [3]. It is expected for the coming 5G networks to be able to autonomously access the most pertinent spectral widths, through sophisticated and efficient learning and inference mechanisms, to control the data transmission power and adjust its protocols to enhance quality [4, 5]. Then, the new challenge is focused on developing intelligent-adaptive learning and the decision making necessary to satisfy all the requirements underlying the next generation networks [6].

AI can help us foresee the operation complexity of the future networks giving us new sources to implement an intelligent use of the computational resources with an improved context conscience [7, 8], furthermore, AI can also concede final users with a better distribution for computing, storage, control and communication functions [9]. Currently, AI techniques are combined with the management and control of the coming networks' generation, for example, Kato et al. [10] used the deep learning technique to improve the heterogeneous network traffic control by proposing a surveyed deep learning system, that is trained based on characterized input using borderline router traffic patterns, showing great effectiveness and an improvement over the OSPF routing method.

The automated learning AI approach has the capacity to provide simpler solutions to complex problems through a short period analysis to great data volumes by adapting its functions to variable environments and predicting future events with reasonable accuracy [11, 12]. Among the different functions to control and manage the new coming 5G networks: planning, design, management, monitoring, failure detections, and security (fundamental in nowadays world) [13]. It is the latter upon which this research will be focused on, by using automated learning through deep neural networks and cluster' analysis to group users and devices; to detect malicious signs, intruders [11, 14], anomalies, and failures; and to classify users' behaviors [4].

2. Related Work

Yang et al. [15] found that to approach 5G Networks it was necessary to use automated learning techniques based on Deep Reinforced Learning (DRL), in which a cellular interruption in the UDN is proposed, to maximize the aggregate of performance while satisfying the quality standards for all mobile network users. To achieve such results compensation users were aggregated to the adjacent BS, using a Kmeans algorithm and a deep neural network, to estimate the action-value function. From this research, we found valuable the initial user grouping method used to route them to the closer signal generation source.

5G networks have been predicted to be chaotic and unpredictable and it is crucial to guarantee the highest security in the access points, therefore, efficient user classification and grouping are fundamental [16]. One plausible solution in

this respect is a network perimetric and dynamic grouping, achieved through DRL using a Deep Q-network (DQN) model, that responds better as a cluster and has proven itself to be more efficient than a static reference [17].

Yang et al.[18] proposed a combined intrusion detection model, based on deep learning, to detect any intrusive behavior inside a network. This model was generated from a database containing characteristics' mapping, one-hot encoding, and normalization processing that are loaded into a DBN, which uses a Boltzman machine (RBM) connected to a BP neural network on its auxiliary layer to precisely adjust its weighing and an SVM to train the detection method. This DBN-SVM detection method was tested, and its experimental results show an outstanding performance to pin out intruders. Similarly, Mehmood et al. [19] used a characteristics database by Cluster heads (CH) to block repetitive malicious activity on wireless sensor networks, prone to security bridges, using a system generated from a knowledge set to classify the events taking place in the network nodes. Through this system, there is a performance load lessening on the nodes due to the action of the Cluster Heads that register the hazard level of the intruding nodes through an inference motor; such effect, which is not focused on the security scheme of the nodes themselves, can be transposed to this research that is focused on the final users in conjunction with a non-robust deep learning algorithm applied to only one of the network nodes.

Zhang et al. [20] generated an accurate classifier focused on Access Network Intruder Detection (ANID) using a particle swarm optimization algorithm suited for SVDD parameters and tested with UCI and KDD99 datasets. The results show greater accuracy in classification and lower false-alarm rates when compared with traditional approaches; this effect can be associated with the use of optimization algorithms improved with deep automated learning networks.

Sedjelmaci [21] presented an intelligent cybersecurity scheme to provide protection to 5G networks, through detection systems located at various critical points of the network that identify any intrusion with malicious behavior. Hierarchical Reinforcement Learning (HRLD) algorithms are implemented that allow systems to collaborate with each other to improve their attack detection accuracy over time, the results show that the scheme detects attacks more accurately when the number of iterations is increased, which closely resembles DDoS-type attacks. Similarly, the researchers propose an approach known as multilayer intrusion detection and prevention (ML-IDP), which provides the necessary security in 5G networks enabled for SDN / NFV deployed in the cloud, through the timely detection of attacks [22]. The system consists of five layers where algorithms such as Four-Q-Curve are used for user authentication, game theory and deep reinforcement learning to protect the network switches, Shannon Entropy to classify incoming packets into two classes: normal and suspects and increased multiple SOMs to address dangerous packets.

To control 5G networks access effectively this research implements the access control that identifies the closer actors to the access point proposed in [15, 23]; the user classification (allowed and possibly hazardous) through a deep learning network model established in [17, 24]; and the access security workflow and deep learning networks implementation, based on a Characteristics Database and the use of deep neural networks focused on the final user, developed in [18-20] respectively.

A summary table of the related works reviewed is presented, pointing out the advantages and limitations they present for the research in Table 1.

Table 1. Related works analysis.

Research	Analysis
[15]	It presents a contribution in the initial user grouping method used to route them to the closest signal generation source, as well as the use of deep learning as a method of approach to 5G networks. On the other hand, the work is limited to maximizing the performance of all users accessing the network and at the same time satisfying the quality of service demands of each mobile user. Furthermore, there is no proposal in terms of security.
[17]	A dynamic and perimeter network clustering is proposed, this using DRL and a DQN model to ensure efficient and secure data transport and meet the load balancing requirements of edge servers. It presents good results in terms of efficiency in perimeter computing applied in IoT networks, not knowing its impact on other types of networks.
[18]	The deep learning-based intrusion detection model presented in this research to detect any dangerous behavior within a network is highly efficient and provides important information for the development of the 5GDoSec model, however, its scope is limited to wireless networks. traditional, which prevents verifying its operation in other types of networks such as 5G.
[19]	This work uses Cluster Heads (CH) through a security system generated from a set of event classification knowledge, to block malicious activities on the network. The use of clusters to identify threats is an effective element that presents high performance and for this reason, it is considered for the development of the 5GDoSec model. Although the results of the implemented system are favourable, its operation is limited to wireless sensor networks.
[20]	The proposed classifier, focused on the detection of intrusions in the access network (ANID), presents a great performance in terms of classification precision, however it does not contemplate its operation in 5G networks.
[21]	Hierarchical reinforcement learning algorithms (HRLD) are a great alternative to provide general security in 5G networks in terms of intrusion detection, allowing to provide the necessary security to connect with multiple services. The results obtained can generate other performance values with the use of other algorithms for the implementation of the system and focusing specifically on DoS attacks.
[22]	It covers several security vulnerabilities in 5G networks that are highly exploited with the use of common IDPS, preventing attacks such as IP spoofing, flow table overload, DDoS and hijacking of the host location among others, however, the scheme is implemented specifically for SDN, NFV and cloud technologies, which limits its field of action, preventing its application in other types of possible scenarios.

3. Methodology and Design

The selected methodology for this research follows an evolutive process based on a prototyping model consisting of 5 stages to rapidly develop a software proposal to address the security access protocol for 5G networks: communication, quick planning, quick design and modeling, construction and implementation, and delivery and feedback (Fig. 1).

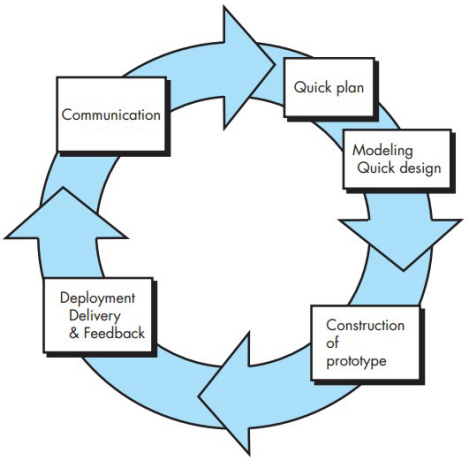

Fig. 1. The prototyping paradigm [25].

After the communication stage (solution proposal), an initial implementation plan is defined to define a dataset and use a machine learning technique to group and classify the data in two outputs: hazardous or allowed users. The design will be based on the data of the users of a 5G network [26], in this case, a set of data for predicting behaviors in 5G networks. The design and construction stages are done using automated learning algorithms that are to classify the users through the knowledge gained from administrator authorizations and the behavior patterns considered not-dangerous as shown in Fig. 2. Finally, the 5GDoSec model is tested using a monthly dataset not used for previous training, if any addition or verification is needed a re-training process is done using new data for authorized and malicious users as well as new behavior patterns.

Fig. 2. Base station deployment.

3.1. Dataset

The data set used for the development of this research (5g-user-prediction) contains information about access by users to different types of networks, including the 5G network, registering their id, area id (An alphanumeric value initiated by the "V0" indicator), id of the provider (An integer between 10 to 97), type of channel service (An integer between 1 to 10 that indicates the type of channel service), type of service (An integer between 1 to 5 that indicates the type of service), type of product (An integer between 2 to 5 that indicates the type of product analysed), total connection time, activity carried out per day and if it is a 5G network or not, among others [26].

The fields of the data set provide the necessary information so that it is possible to find a cluster that relates a user to the amount of activity carried out and the total connection time. In this way, malicious network access can be detected and prevented in time using unsupervised machine learning techniques. The fields used in the implementation of the model are listed below:

- User ID (32 hexadecimal alphanumeric values).
- Total connection time (An integer between 0 to 200.841).
- Activity performed per day (23 days logged per user, An integer between 0 to 30).
- It is a 5G network (A numerical value 1.0 or 0.0).

3.2. Data preprocessing

A data preprocessing process is carried out first by making a selection of the records that correspond to 5G networks, obtaining a total of 9273 records, 50% for training and 50% testing, then a grouping of activity per day is performed, where a new feature is created that contains the sum of all the activity carried out by the user during the registered days and finally a normalization process is carried out for the fields in the range between 0 and 1.

3.3. Self-organizing map (SOM) neural network design

A deep neural network (Fig. 3) is developed in MATLAB [27] to determine a cluster set, to classify users into permitted and hazardous, using auto-supervised learning techniques. The inputs of the neural network are two: total connection time and total active days and de outputs are the corresponding clusters. Having acquired the necessary data the self-organizing map master network (Fig. 3) for the clusters is created; the neural network (5×5) consists of the input and twenty-five outputs or classification clusters (one of these will hold the negated or untrustworthy elements).

The security rubric was defined as a user who has many accesses in a short period of time must be classified as a dangerous user. The number of clusters are used considering the complexity behind the rubric defined to simplify the system as needed and the values can be incremented if greater or more precise classification capacity is required.

Based on the deep neural networks and a specific layer with an auto-organizational map [28] the 5GDoSec model aims to classify the input data into clusters (Fig. 4): permitted users and non-permitted or hazardous users.

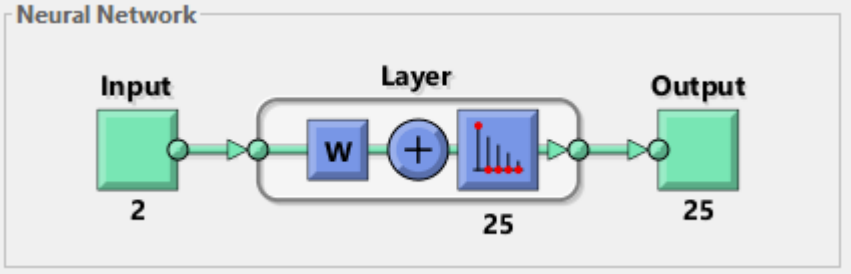

Fig. 3. Neural clustering design.

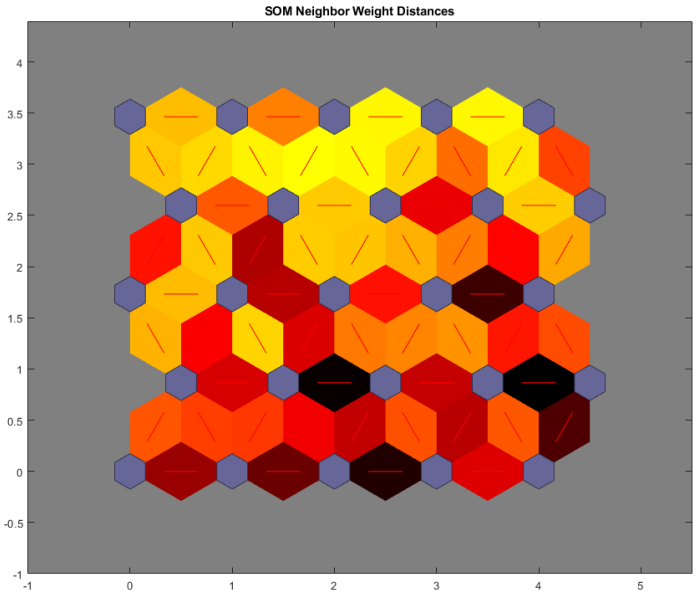

Fig. 4. Clusters' design.

3.4. Model design and security Policy

Security analysis is based on the DoS attack and service denegation variables [29], therefore, specific rubrics were designated for user classification: a user who has many accesses in a short period of time must be classified as a dangerous user.

The model structure is shown in Fig. 5 where the inputs are an user database that contains user ID, total connection time and total activity performed per days, the model process is implement SOM clustering techniques on the user records to group them into the established categories: permitted users and non-permitted or hazardous users and the model outputs are a cluster with non-permitted or hazardous users.

The proposed security policy would dictate to "allow the access to the users grouped in the trusted cluster and reject the users in the possibly hazardous cluster", using Access Control Lists (ACL) to restrict the access to the non-trusted users to the network and limit the traffic coming from their IP addresses [30, 31].

The security system used by the model is shown in Fig. 6, where the outputs of the model check if a user is in the group of users not allowed, if so, an expert performs an evaluation of whether it is misclassified or not no, and if so, a retraining of the model is requested to classify the user as trustworthy.

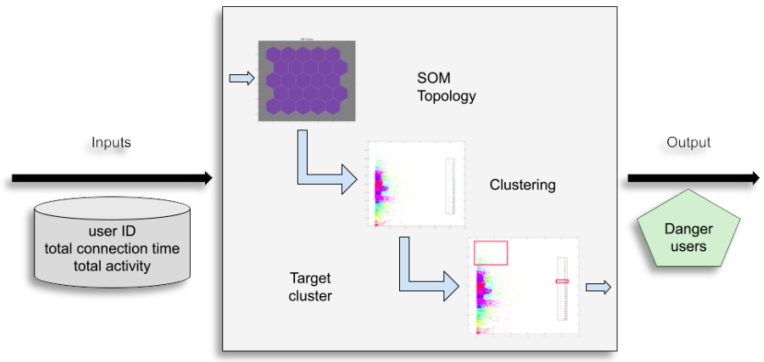

Fig. 5. Security model.

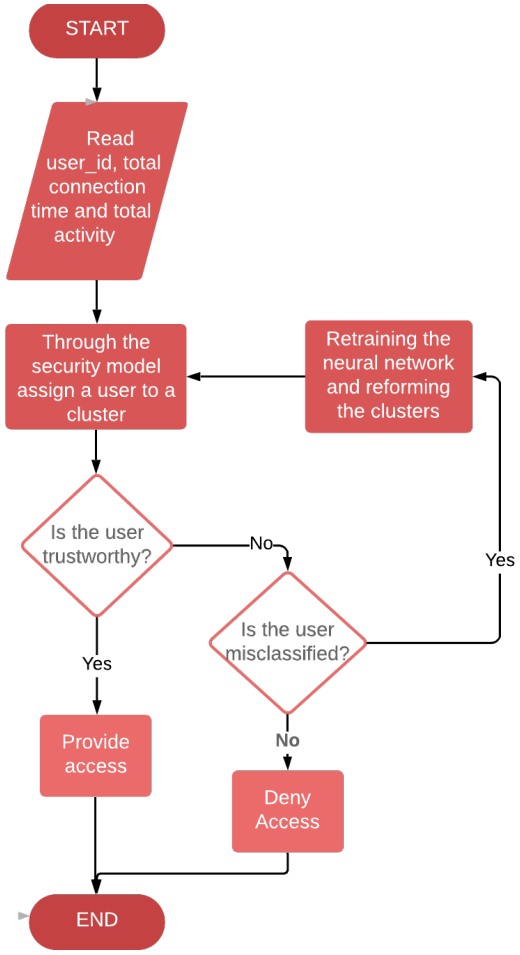

Fig. 6. System flowchart.

3.5. Simulation environment

The simulation, construction and testing tool for the security model is Matlab version R2021a, using the data set described above and the functions of the Deep Learning Toolbox product selforgmap, plotsomhits, plotsompos and evalclusters, the latter using the DaviesBouldin metric [32], and comparing the results obtained with traditional clusters such as Kmeans and Linkage.

For the training and model configuration phase, 50% of the data, that is 4637 records, was used and for the testing and validation phase, the remaining data was used. The selection of the records for each dataset was done randomly.

4. Results and Discussion

For a correct implementation of the model (Fig. 5) it is necessary to acquire a database containing trustworthy and potentially hazardous users as well as a neural network to classify them in clusters considering their behavior within the network: total connection time and total activity. Afterward, the development is divided into two stages; a training stage in which the algorithm's neural network is trained to create the clusters and an initial users' database; and the verification and testing stage in which, according to the output from the previous stage, an initial test is carried out using a new dataset.

4.1. Training stage

As outputs of the training stage, the classification neural network groups are defined, and the total connection time of the dataset and the total activity are entered as inputs. The neural network is trained using the processed dataset (4637 registers), after 200 training cycles the network is ready to carry out the users' classification; the self-organizing map obtained shows a 25 adjacent cluster typology (Fig. 7) where about 50% of the clusters contain 70% of the data and the others can be analysed for potentially dangerous network behaviour.

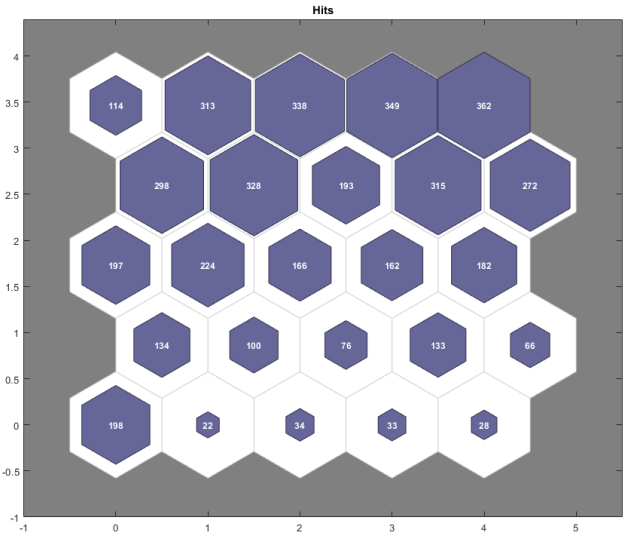

Fig. 7. Sample topology training.

Cluster 10 was selected to house the potentially dangerous users with 66 entries, as shown in Fig. 8, the coverage area of the weight position contains the points that allow a good classification into dangerous users according to the security rubric.

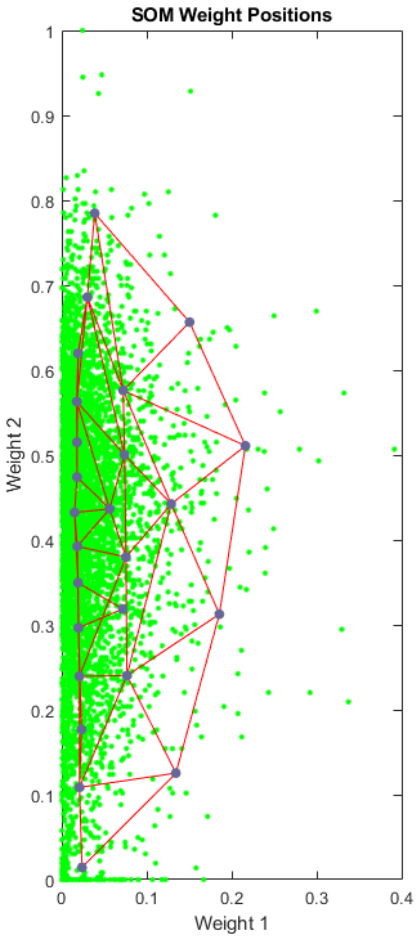

Fig. 8. Self-organizing map weight positions.

Once the classification clusters within the SOM have been established, the next stage consists of creating the database of trusted and untrusted users: based on the results shown in Figs. 7 and 8, the behaviour of the users in cluster 10 is evaluated, showing in Fig. 9 that they have the highest number of entries in very short periods of time, therefore these users will be classified as potentially dangerous according to the previously defined security rubric. The final set of results for possible dangerous users contains 66 of the 4367 entries, so these users are included for processing in the ACLs of each AP.

The DaviesBouldin metric is used for clustering validation where its value is compared in Table 2, using traditional Kmeans and Linkage clustering techniques for user classification, obtaining a value of 0.7873 for SOM, showing the best performance.

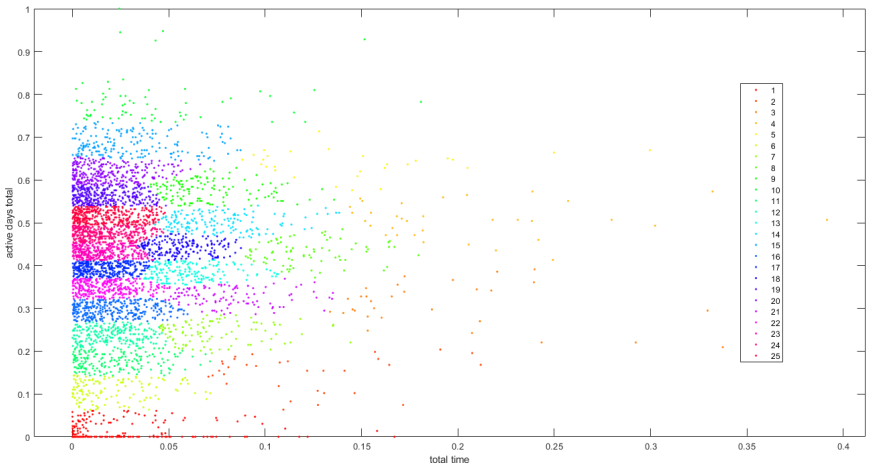

Fig. 9. Cluster scatter plot training.

Table 1. DaviesBouldin criterion value for training.

Clustering technique	DaviesBouldin criterion value
SOM	0.7873
Kmeans	0.8040
Linkage	0.8846

4.2. Verification stage

To proceed to the verification stage, we used the remaining dataset, which was processed in the same way as the previous stage with a sample of 4636 entries. As shown in Fig. 10, 67 entries were classified in cluster 10 as possible dangerous users, which are referred for restriction in the ACLs. It is also noted that the proportion of hazardous user classification is maintained at around 1.4%.

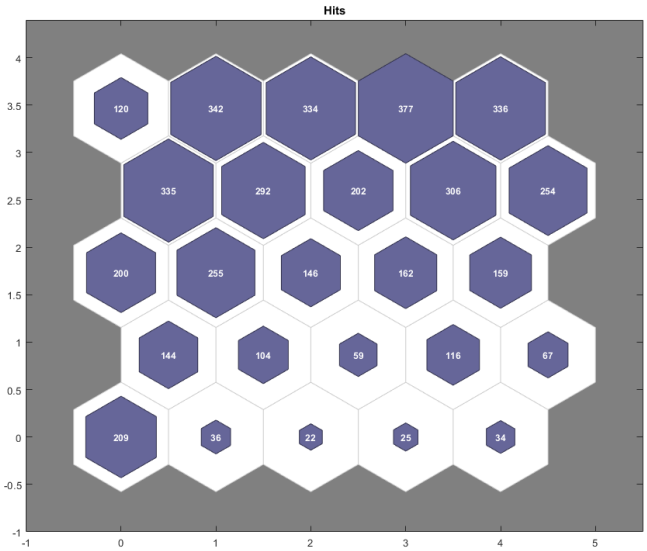

Fig. 10. Sample topology testing.

All users into cluster 10 are added to the possibly hazardous database, 67 users for this dataset. If needed, the behavior of the newly added users can be verified, and their records can be deleted once they are validated as trustworthy. As shown in Fig. 11, it can be seen that the users classified in cluster 10 maintain the behaviour that has been marked as dangerous: many accesses in short periods of time.

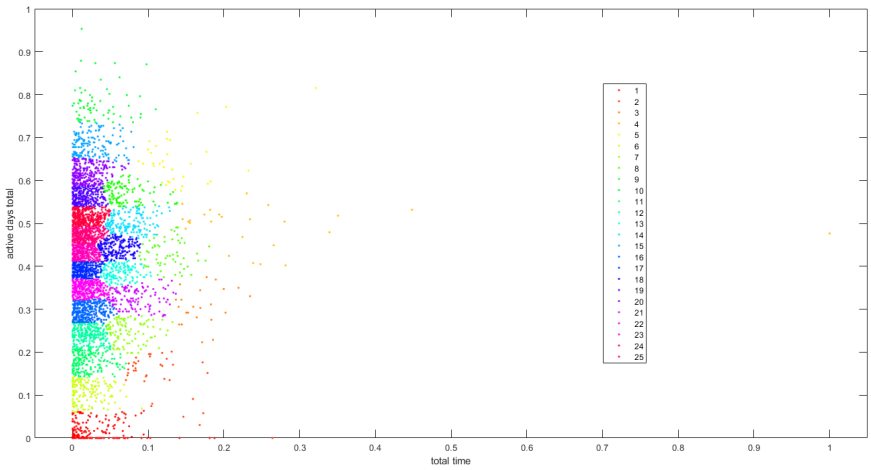

Fig. 11. Cluster scatter plot training.

The DaviesBouldin metric shows the validation of the clustering where its value is compared in Table 3, obtaining a criterion value of 0.8177 and a difference with training of 0.0304 for SOM, showing the best performance.

Table 2. DaviesBouldin criterion value for testing.

Clustering technique	DaviesBouldin criterion value	Difference with training
SOM	0.8177	0.0304
Kmeans	0.8682	0.0642
Linkage	0.9739	0.0893

5. Conclusions

The proportion of users classified in each cluster follows the same pattern established in the training stage according to the weight positions within the self-organising map, therefore, users that are untrusted and most likely to be part of DoS attacks are grouped in cluster 10 while the other clusters host the trusted addresses.

The results obtained show a reliable prototype, following the parameters established in the security rubric, to classify potentially dangerous users, direct them to the cluster determined in the SOM, add their records to a database for ACLs in each AP, and null their data traffic within the network.

The model validated its clusters in the training and testing phases show a better performance in SOM in contrast to other techniques such as Kmeans and Linkage, besides being an unsupervised learning strategy allows the classification of users

without knowing any prior information about them except for the inputs required by the model, which can be obtained from a simple analysis of the network traffic.

The storing of the potentially hazardous users in an independent database allows a computational wear-off diminishment, using ACLs with low complexity management, in the access devices associated with the prevention and detection of possible intruders.

6. Future Work

The successful implementation of non-supervised learning methods, through clustering techniques in neural networks, for 5G networks, opens the door to rubrics' comparison regarding access security, computing speed, and performance across different 5G environments also the low size of the neural network allows it to be stored in low capacity devices and to be embedded as a programmed task within the network or into each AP.

The proposed model can be studied using other types of distributions for access control in wider 5G networks. Locating it at strategic access points in the network or at switches is an alternative that can be implemented using techniques such as software-defined networking (SDN) or network functions virtualisation (NFV).

References

1. Le, L.-V.; Lin, B.-S.P.; Tung, L.-P.; and Sinh, D. (2018). SDN/NFV, Machine learning, and big data driven network slicing for 5G. *Proceedings of the* 2018 *IEEE* 5*G World Forum* (5*GWF*), Silicon Valley, USA, 20-25.
2. El Azzaoui, A.; Singh, S.K.; Pan, Y.; and Park, J. H. (2020). Block5GIntell: blockchain for AI-Enabled 5G networks. *IEEE Access*, 8, 145918-145935.
3. Kibria, M.G.; Nguyen, K.; Villardi, G.P.; Zhao, O.; Ishizu, K.; and Kojima, F. (2018). Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. *IEEE Access*, 6, 32328-32338.
4. Jiang, C.; Zhang, H.; Ren, Y.; Han, Z.; Chen, K.C.; and Hanzo, L. (2017). Machine learning paradigms for next-generation wireless networks. *IEEE Wireless Communications*, 24(2), 98-105.
5. Yi, H. (2021). Improving security of 5G networks with multiplicative masking method for LDPC codes. *Computers and Electrical Engineering*, 95, 107384.
6. Kumar, N.H.; Baskaran, S. (2019). Machine learning: The Panacea for 5G complexities. *Journal of ICT Standardization*, 7(2), 157-170.
7. Chen, M.; Challita, U.; Saad, W.; Yin, C.; and Debbah, M. (2019). Artificial neural networks-based machine learning for wireless networks: A tutorial. *IEEE Communications Surveys & Tutorials*, 21(4), 3039-3071.
8. Gutierrez-Estevez, D.M.; Gramaglia, M.; De Domenico, A.; Dandachi, G.; Khatibi, S.; Tsolkas, D.; Balan, I.; Garcia-Saavedra, A.; Elzur, U.; and Wang, Y.(2019). Artificial intelligence for elastic management and orchestration of 5G networks. *IEEE Wireless Communications*, 26(5), 134-141.
9. Bogale, T.E.; Wang, X.; and Le, L.B. (2018). Machine intelligence techniques for next-generation context-aware wireless Networks. *ITU Journal: ICT Discoveries*, Special Issue(1), 109-119.

10. Kato, N.; Fadlullah, Z.M.; Mao, B.; Tang, F.; Akashi, O.; Inoue, T.; and Mizutani, K. (2017). The deep learning vision for heterogeneous network traffic control: proposal, challenges, and future perspective. *IEEE Wireless Communications*, 24(3), 146-153.
11. Kafle, V.P.; Fukushima, Y.; Martinez-Julia, P.; and Miyazawa, T. (2018). Consideration on automation of 5G network slicing with machine learning. *Proceedings of the* 2018 *ITU Kaleidoscope: Machine Learning for a 5G Future* (*ITU K*), Santa Fe, Argentina, 1-8.
12. Tsai, C.-W.; Chen, Y.-P.; Tang, T.-C.; and Luo, Y.-C. (2021). An efficient parallel machine learning-based blockchain framework. *ICT Express*, 7(3), 300-307.
13. Fang, D.; Qian, Y.; and Hu, R.Q. (2017). Security for 5G mobile wireless networks. *IEEE Access*, 6, 4850-4874.
14. Parwez, M.S.; Rawat, D.B.; and Garuba, M. (2017). Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. *IEEE Transactions on Industrial Informatics*, 13(4), 2058-2065.
15. Yang, X.; Yu, P.; Feng, L.; Zhou, F.; Li, W.; and Qiu, X. (2019). A Deep reinforcement learning based mechanism for cell outage compensation in 5G UDN. *Proceedings of the* 2019 *IFIP/IEEE Symposium on Integrated Network and Service Management* (*IM*), Arlington, USA, 476-481.
16. Ahmad, I.; Yau, K.L.A.; Ling, M.H.; and Keoh, S.L. (2020). Trust and reputation management for securing collaboration in 5G access networks: The road ahead. *IEEE Access*, 8, 62542-62560.
17. Liu, Q.; Cheng, L.; Ozcelebi, T.; Murphy, J.; and Lukkien, J. (2019). Deep reinforcement learning for IoT network dynamic clustering in edge computing. *Proceedings of the* 2019 19*th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (*CCGRID*), Larnaca, Cyprus, 600-603.
18. Yang, H.; Qin, G.; and Ye, L. (2019). Combined wireless network intrusion detection model based on deep learning. *IEEE Access*, 7, 82624-82632.
19. Mehmood, A.; Khanan, A.; Umar, M.M.; Abdullah, S.; Ariffin, K.A.Z.; and Song, H. (2017). Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access*, 6, 5688-5694.
20. Zhang, C.; Ni, M.; Yin, H.; and Qiu, K. (2018). Developed density peak clustering with support vector data description for access network intrusion detection. *IEEE Access*, 6, 46356-46362.
21. Sedjelmaci, H. (2021). Cooperative attacks detection based on artificial intelligence system for 5G networks. *Computers & Electrical Engineering*, 91, 107045.
22. Abdulqadder, I.H.; Zhou, S.; Zou, D.; Aziz, I.T.; and Akber, S.M.A. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Computer Networks*, 179, 107364.
23. Moysen, J.; Giupponi, L. (2018). From 4G to 5G: Self-organized network management meets machine learning. *Computer Communications*, 129, 248-268.
24. Maksymyuk, T.; Šlapak, E.; Bugár, G.; Horváth, D.; and Gazda, J. (2020). Intelligent framework for radio access network design. *Wireless Networks*, 26(1), 759-774.

25. Pressman, R.S.; Maxim, B.R. (2019). *Software engineering : a practitioners approach*. McGraw Hill Book Company, Inc.
26. 国企算法选手 (2020). 5g-user-prediction. Retrieved July 16, 2020, from https://www.kaggle.com/liukunxin/dataset?select=train.csv.
27. MathWorks Inc. (2020). Cluster data by training a self-organizing maps network - MATLAB. Retrieved July 16, 2020, from https://www.mathworks.com/help/deeplearning/ref/neuralnetclustering-app.html.
28. MathWorks Inc. (2020). Cluster with self-organizing map neural network - MATLAB & Simulink. Retrieved July 16, 2020, from https://www.mathworks.com/help/deeplearning/ug/cluster-with-self-organizing-map-neural-network.html.
29. Javed, M.A.; Khan Niazi, S. (2019). 5G security artifacts (DoS/DDoS and Authentication). *Proceedings of the* 2019 *International Conference on Communication Technologies* (*ComTech*), Rawalpindi, Pakistan, 127-133.
30. Shirey, R. (2007). Internet security glossary, RFC 4949 Version 2.
31. Bonfim, M.; Santos, M.; Dias, K.; and Fernandes, S. (2020). A real-time attack defense framework for 5G network slicing. *Software Practice and Experience*, 50(7), 1228-1257.
32. Hasanzadeh, K. (2014). *SoftGIS data mining and analysis: A case study of urban impression in Helsinki*. Master's Thesis, School of Engineering, Aalto University.