DoS Attacks Detection in the Network of Drones: An Efficient Decision Tree-Based Model

Tarek Gaber[1,2(✉)], Xin Fan Guo[3], and Said Salloum[1]

[1] School of Science, Engineering, and Environment, University of Salford, Salford, UK
t.m.a.gaber@salford.ac.uk
[2] Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt
[3] Faculty of Natural, Mathematical and Engineering Sciences, Department of Informatics, King's College London, London, UK

Abstract. This study examines the detection of the denial of service (DoS) attacks on Wi-Fi-based unmanned aerial vehicles (UAV). The paper proposed an efficient DoS attack detection method based on Decision Tree classifier. The method consists of preprocessing, feature extraction, and DoS attack detection. The preprocessing was proved to save drones' resources and improve the detection rate. The investigation of different classifiers, i.e., KNN, Random Forest, Logistic Regression, and Decision Tree, the latter was concluded to be the best in detecting DoS attacks of types of De-authentication and UDP/TCP flood within the shortest runtime. The evaluation further showed that proposed DoS detection method is better than the most related work where it achieved detection with F1-score of 0.989 and with the shortest latency.

Keywords: DoS attack · Smart cities · Machine learning · Decision Tree · Algorithm Latency

1 Introduction

In large-scale and interconnected urban residences, a smart city offers convenient and better-quality services [1]. A smart city may be considered a convergence of a large amount of information and communication technologies to offer services like logistics, traffic management, and goods delivery [2]. This ensures that citizens are offered intelligent, automated, and adaptive services. The smart city worldwide market was found to be around USD 741.6 billion during the COVID-19 crisis in 2020 and was expected to reach USD 2.5 Trillion by 2026 [3]. The rapid increase in digitally-enabled services during the COVID-19 crisis may have occurred because of the ready adoption of technology that allowed the masses to access services remotely [2]. However, such adoption could be hindered if the most common cybersecurity attacks such DoS [4] and phishing [5] are not detecting.

Various traditional services may be included in a smart city, which can be automated and delivered using Artificial Intelligence (AI)-based decision-making [6]. For example,

R. Hou et al. (Eds.): BDTA 2021/2022, LNICST 480, pp. 169–178, 2023.
https://doi.org/10.1007/978-3-031-33614-0_12

real-time traffic data that is obtained from different localities within a smart city can be provided to a traffic light, which leads to intelligence and adaptive signal transition timings and thus, improved traffic flow and reduced possibility of a traffic jam. In the same way, it is possible to transform a conventional electricity grid into a smart electricity grid that provides real-time energy usage information to both the grid operators and end users. It is expected that by 2026, the smart energy segment will attain a global market value of USD 652.9 billion [2, 3].

Various operations can be carried out by Unmanned Aerial Vehicles (UAV), which is an enabling technology, such as agriculture, rescue, delivery, inspection and, catastrophe response. Popularly known as drones, UAVs are a developing facilitator of various smart city services. A ground controller unit is used to control UAVs that usually offer services like observing weather phenomena, product delivery, aerial photography, and surveillance. UAVs also include remotely operated and unmanned flights, like the S-100 Camcopter, that carry defense service payloads to remote and hard-to-reach areas [7]. There is clearly a rapid spread of drones in the commercial markets, with its market share expected to become USD 58.4 billion by 2026 [2, 7]. Though it was used as a military vehicle initially, at present, it is increasingly used in commercial and consumer machines. Ensuring secure and reliable functioning is a key issue for the universal presence of UAVs. Cyber threats (such as GPS spoofing, data leakage, and flight disruption) exist, which can have an impact on these vehicles, generating unexpected situations that may be dangerous for stakeholders (such as operators, ground stations, and the general public) that are part of the operational environment [4, 7, 8].

As explained previously, there are several advantages of incorporating drones within a smart city. However, no universal and comprehensive model is developed for determining, avoiding, or even identifying cyber threats that are faced when drones are introduced in a smart city's airspace. Public safety is compromised when drones enter into no-fly zones, putting a secure premise at risk, such as entering an airport's airspace and putting aircraft and airport operations at risk, as well as the dropping of illegal products (such as delivering unlawful goods to prisons). Recent years have seen considerable developments in research and development in this field [2, 4, 9]. An AI-enabled portable drone detection unit (tower) has been presented by Dedrone for identifying unlawful drone intrusions into no-fly zones by installing monitoring towers in particular areas [2, 10].

Though there is a rapid development in the existing research about cyber-attacks involving drones, it is still needed to investigate drone-based cyber-attacks, evaluate the kinds of threats faced by a smart city's airspace, and how a city's economy is affected by a drone-based attack. For example, Denial of Service (DoS) attack could lead to operational disruption in a network of drones. One of the widely used platform controlling Wi-Fi-based UAVs is the Parrot AR Drone 2.0 as its documentation is extensively available and not expensive [11].

The authors in [4] proposed a DoS attack detection model using machine learning with high accuracy results reaching 99. However, from analyzing the dataset used in [4], it was noticed that there are duplicates of 32.17%, Fig. 2 shows an example of duplicate entries. Such duplication would lead to unreliable outcome, i.e., unreliable DoS detection rate which could have massive loss, e.g., unresponsive drone. This also leads to more

power consumption which is limited in drone's environment. This paper aims to address these problems by proposing an efficient DoS attack detection with high detection rate.

The structure of the rest of the paper is as follows. The related work is discussed in Sect. 2 which is followed by an overview of the Denial of Service (DoS) attack in Sect. 3. The proposed method is presented in Sect. 3. In Sect. 4, the results and discussion are given. Finally, conclusions and some further work are highlighted in Sect. 5.

2 Related Work

As one of the widely available commercial quadcopter platform for controlling UAVs [11], the Parrot AR. Drone 2.0 has been subject to various security investigation studies which identified many security flaws. This platform is for many UAV activities including packet inspection, operating system assessment to identify active programs and file readers, as well as port scanning to look for accessible services. As reported by Hooper et al. [12] Buffer overflow, DoS, and ARP cache poisoning were effective attacks against the platform. To protect Wi-Fi-based commercial UAVs, it also proposes a multi-layer security method to tackle flaws on the so-called aerial computers, however, it does not offer any prevention for the breakthroughs or the subsequent actions to protect the existing susceptible system.

Pleban et al. [13] proposes a fortification process for the UAV to address the flaws. For instance, it advises altering the Wi-Fi communication protocol to include encryption and authentication. But this moderation does not address DoS attacks. The Parrot AR. Drone contains security issues, according to Pleban et al. [13], who also add that this UAV platform is widely used because of its affordable price point.

Gudla et al. [14] have novel suggestions for Parrot AR. Drone's. They proposed a layer between the controller and the UAV called single-board computer (SBC), particularly a Raspberry Pi 3. This SBC provides communication encryption and shifting target protection strategies in addition to a Kismet IDS. Nonetheless, there are no indications of how to apply their findings to protect against DoS in that scenario. As prevention for the security flaws which is a legacy system update, Astaburuaga et al. [15] propose a security evaluation for Parrot AR. Drone 2.0. However, the DoS is not resolved considering the excellent protection provided for other weaknesses.

The computational cost of traditional IDSs makes them impractical in UAVs context. Machine learning (ML) based approaches proved be effective in detecting different sort of attacks [16, 17]. Given the complex and dynamic nature of UAV systems' security domain, which is comparable to that of the intrusion detection system (IDS) sector, a lot of data analysis is necessary to categorize these security-related occurrences.

According to Sommer & Paxson [18], there are certain difficulties with using ML to IDS. Due to its inherent capacity to train from data and make judgments based on that learning, ML has been employed in a variety of disciplines in the past, including spam detection and object detection [19]. It contrasts the traditional employment of machine learning (ML) for classification issues with instances of misuse and anomaly identification needed for cyberattacks. Anomalies are deviations from regular conduct, while misuse is predicated on known malevolent conduct. It must be noted that ML outperforms in classifying recognized attacks (already trained - misuse) than it does

in detecting unidentified malicious occurrences (anomalous). According to Sommer & Paxson [18], the enormous influence of untrue events in the security sectors, taken as not malicious can result in cataclysmic events for our application, as opposed to the influence on more traditional ML systems such as spam classifiers, where a false-negative will merely be bothersome.

The authors in [4] proposed a DoS attack detection model using machine learning with high accuracy results reaching 99. However, from analyzing the dataset used in [4], it was noticed that there are duplicates of 32.17%, Fig. 2 shows an example of duplicate entries. Such duplication would lead to unreliable outcome, i.e., unreliable DoS detection rate which could have massive loss, e.g., unresponsive drone. This also leads to more power consumption which is limited in drone's environment. So, his paper aims to address these problems by proposing an efficient DoS attack detection with high detection rate.

3 Overview of Denial of Service Attack

The reliability of the systems, e.g., UAV's systems, is hampered by Denial of Service (DoS) attacks. An effective DoS attack causes a communication or control failure on the target UAV systems causing major consequences.

- **TCP and UDP Flood**

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two widely employed protocols for data transfer via networks. The primary distinction between them is that TCP employs feedback packets to ensure error correction, packet ordering, and data transmission between transmitter and receiver. On the other side, UDP lacks TCP-specific "reliability" characteristics. Since there is no need for communication cost, UDP has benefits above TCP in terms of the velocity of communication between the controller and the system.

On port 5555 for streaming video and port 5559 for optional control and crucial data, the TCP protocol is employed. Just on Parrot AR. Drone 2, the UDP protocol is employed to transmit navigational data (status, location, speed, engine rotation speed, among others) on port 5554 and control data (referred to as AT commands) on port 5556. Delivering many packets using both transfer protocols to one of these ports is a flood attack. This enormous number of packets overwhelms the UAV's computing power and causes it to become inaccessible, which is known as a Denial of Service (DoS) Attack.

- **De-authentication Attack**

To conserve computing services, this sort of frame enables the point of access or the client linked to the access point to ask for its de-authentication. De-authentication is a feature of the IEEE 802.11 standard that belongs to the group of control packets. Malicious agents have taken advantage of this feature by pretending to be a valid client and asking for a de-authentication to the access point.

Consequently, a security technique that can recognize and disregard these malicious packets without removing their usefulness is needed. The IEEE 802.11 protocol offers no security protection against these spoofing attacks. Due to the absence of connectivity

between the controller and the UAV throughout this de-authentication attack on the Parrot AR. Drone, a devastating collision into external obstructions while the flight is likely to occur.

4 Proposed DoS Attack Detection Method

The proposed method consists of three phases as given in Fig. 1: preprocessing, feature extraction, and DoS attack detection. In the preprocessing, from analyzing the dataset [4], it was noticed that there are duplicates of 32.17%, Fig. 2 shows an example of duplicate entries. Such duplication would lead to unreliable outcome, i.e., unreliable DoS detection rate. Table 1 shows a summary of the dataset after cleaning it where it can be noticed that 32.17% has been removed thus minimizing the processing time.

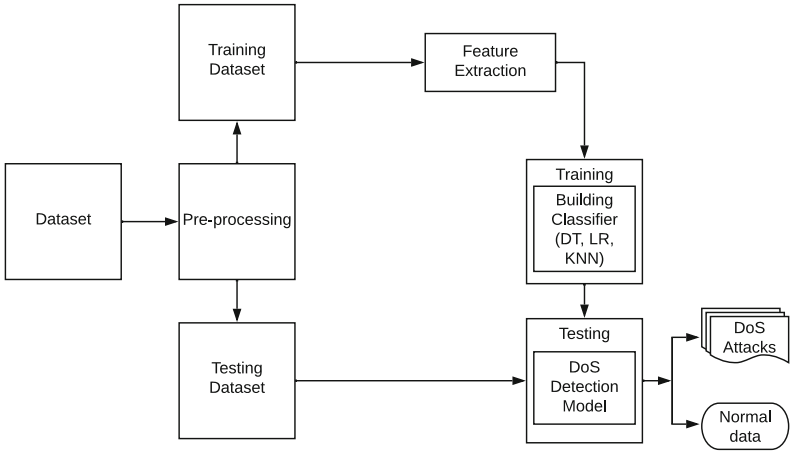

Fig. 1. DoS Detection Model in Drones.

The data was cleaned, i.e., deleting duplicates, using the Python function– *TimeDelata and Bytes(size)*. In the feature extraction phase, as reported by [4], it was tested that the best features to distinguish between DoS data and normal traffic are *Time delta from the previously captured frame (seconds)*, and *Frame Length (bytes)*. In this paper, we also used these two features in the classification phase. In the third phase, ML-based models were trained and tested using the dataset cleaned and built in this first and second phases. In this phase, different classifiers ware evaluated to build the most efficient one addressing the environment of the network of drones. Namely, the Decision Tree (DT) [2], Logistic Regression (LR) [3], KNN and Random Forest were used. Also, like [4], the test/train ratio was 4/6.

5 Results and Discussion

In this section, we discuss how the proposed model was evaluated. It starts with describing the dataset, then discussing the results of the scenarios under which the model was tested and finally the latency analysis of the model. All the experiments of this study were

	Protocol	Bytes	TimeDelta	DestPort	SrcPort	Class
340800	tcp	129	0.000001	NaN	NaN	normal
361715	tcp	129	0.000001	NaN	NaN	normal
319743	tcp	129	0.000001	NaN	NaN	normal
343401	tcp	129	0.000001	NaN	NaN	normal
316110	tcp	129	0.000001	NaN	NaN	normal

Fig. 2. Example of duplicate entries.

Table 1. Data statistics before and after cleaning.

	Number of entries	Normal traffic	De-auth attack	UDP flood	DoS TCP
Before	474311	459839	8576	5493	403
After	321744	307607	8282	5478	377

conduct under the following specifications: MacPro with Intel(R) Core(TM) i9-9980HK CPU 2.40GHz and the code was written using Python Python 3.10.2.

5.1 Dataset

To evaluate the proposed DoS detection method, the dataset, collected and described in [4], was used. The dataset was collected under the setting that Parrot AR.Drone 2.0 platform was controlling Wi-Fi UAVs. The attacks (De-Authentication Attack and TCP/UDP Flood) data were collected using aircrack-ng tool [20] used and hping3 tool [21] respectively. The normal data were collected under three scenarios: landing and takeoff command, UAV handshakes and Controller, and aleatory flight (multiple non-deterministic routes). The total number of rows of the dataset is 474311 (459839 of normal traffic, 8576 of De-auth attack, 5493of UDP floodand 403 of TCP flood). The evaluation of the proposed DoS detection method was evaluated using three main scenarios as follows.

5.2 Scenario 1: Impact of Data Cleaning on Performance

The aim of this experiment is to investigate whether cleaning the dataset would improve the performance of the modules used in the most related study [4]. So, the Decision Tree (DT) [2] and Logistic Regression (LR) [3] were used. Also, like [4], the test/train ratio was 4/6. The runtime was measured by 7 runs (100 loops each). The parameters values of DT were Criterion = Gini, Max depth = 3. From the results presented in Table 2, it can be noticed that cleaning the data improved the results of DT while only taking 3.81 ms instead of 4.9 for original dataset. It also improved the runtime of LR but not its results.

Table 2. Performance of DT and LR after cleaning the original dataset.

	F1-score	Recall	Precision	Runtime
DT on original dataset	96.8%	99.4%	94.3%	4.9 ms ± 195 µs
DT on cleaned dataset	**96.9%**	**99.4%**	**94.5%**	**3.81** ms ± 101 µs
LR on original dataset	66.9%	59.5%	76.3%	2.02 ms ± 75.5 µs
LR on cleaned dataset	66.8%	**59.7%**	75.9%	**1.68 ms** ± 147 µs

5.3 Scenario 2: Best Value of the DT Parameter "Max-Depth"

In [4], the parameters for the Decision Tree was found using trial and error. The aim of this experiment is to use a more scientific approach to find the optimal max_depth parameter of the Decision Tree which was proven to better than LR in scenario 1 above.

To achieve the desired objective, we have tried different numbers of max_depth while using Gini as the criterion for the cleaned dataset. A summary of the results is given in Table 3 from which it can be seen that the best results (F1-score 98.89%, Precision 98.42%, and Recall 99.36%) were achieved when max_depth was 9 while keeping Criterion = Gini. These results are further improved than the ones in [4] with nearly 2% in F-score.

Table 3. Best value of the DT parameter "max-depth".

Max_depth of DT	F1-score	Recall	Precision
3	96.87%	99.36%	94.50%
5	98.67%	99.84%	97.53%
7	98.87%	99.58%	98.17%
9	98.89%	99.36%	98.42%
10	**98.94%**	**99.49%**	**98.39%**
11	98.87%	99.36%	98.39%

5.4 Scenario 3: Investigating Other Classifiers (KNN and Random Forest)

In this scenario, two more classifiers (KNN and Random Forest, RF) were applied on the cleaned dataset to investigate whether we can get better results. The KNN, as a non-parametric model, was chosen to compare its results with the parametric models such LR. The RF was chosen as it almost has the same parameters as the decision tree. The parameters of LR and DT were the same as the experiments in scenario 1 and 2 where the parameters of KNN and RF were K = 3 and max_depth = 8. Table 4 summarizes the results of Scenario 3.

From this table, it can be seen that the RF results are slightly better than that of DT ones but the later took very long runtime, 472 ns comparing with DT one which is only 3.29 ms. This is expected as the RF needs many trees to get the classification results. So, RF would not be the best algorithm to use in DoS detection in drones' environment which is characterised with limited resources (computation and power).

Table 4. Comparison among DT, LR, KNN, and RF.

	F1-score	Recall	Precision	Runtime
Logistic Regression	66.8%	59.7%	75.9%	1.68 ms ± 147 µs
Decision Tree	**98.94%**	**99.49%**	**98.39%**	**3.29 ms ± 60.6 µs**
KNN	99.0%	99.5%	98.4%	3.5 s ± 103 ms
Random Forest	98.9%	99.5%	98.3%	472 ms ± 30 ms

5.5 Analysis of Model Latency

Because of their embedded nature, UAV applications face the challenges of limited computational capacity and time-sensitive requirements. Thus, unlike the conventional machine learning measures discussed before, latency is an important consideration for these embedded and real-time applications. Therefore, Table 4 displays runtime of the predictions made by each algorithm on a test dataset. It's crucial to note that the testing Latency estimates come from a general-purpose computer, not an embedded one, thus these numbers need to be carefully evaluated. The results show that Logistic Regression is superior to all other algorithms, but its F1-score, recall, and precision are the lowest results. On the other hand, KNN and LR would not be good choices as they took longer time although they produced slightly better results than DT. So, the DoS detection model based on DT is the best choice as it need the lowest latency while still achieve over than 98% in all metrics (i.e., F1-score, recall, and precision). The DT is also good when small dataset is used and all features of this dataset is fed to the classification as in our case explained in the previous sections (Fig. 3).

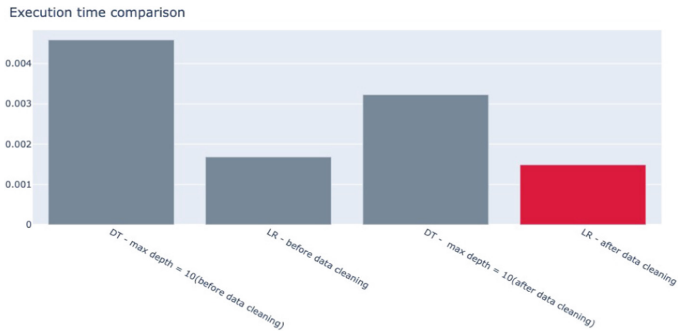

Fig. 3. Execution time comparison.

6 Conclusions and Future Works

The availability of the drones is one of the key issues which should be ensured. DoS attacks are the main threat of the availability services. This paper proposed an efficient and yet accurate DoS attack detection method based on Decision Tree for the Wi-Fi-based unmanned aerial vehicles (UAV). The preprocessing was showed to be very important in minimizing the runtime and algorithm latency which is crucial given the limited resources of UAV-based systems. The experimental results showed that Decision Tree is the best among KNN, Random Forest, and Logistic Regression. The Decision Tree showed to be accurate with F1-score of 0.989 in detecting DoS attacks of types of De-authentication and UDP/TCP flood within the shortest runtime. In the future work, it is planned to collect data for different type of DoS attacks such as spoofing, Sybil and ICMP (Ping) attack.

References

1. Al-Turjman, F., Zahmatkesh, H., Shahroze, R.: An overview of security and privacy in smart cities' IoT communications. Trans. Emerg. Telecommun. Technol. **33**, e3677 (2022)
2. Baig, Z., Syed, N., Mohammad, N.: Securing the smart city airspace: drone cyber attack detection through machine learning. Futur. Internet **14**, 205 (2022)
3. GlobeNewswire: Global Smart Cities Market to Reach $2.5 Trillion by 2026. In: Rep. Link. https://www.reportlinker.com/p05485940/Global-Smart-Cities-Industry.html. Last Accessed 25 Nov 2022
4. de Carvalho Bertoli, G., Pereira, L.A., Saotome, O.: Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle. In: 2021 10th Latin-American Symposium on Dependable Computing (LADC). IEEE, pp. 1–6 (2021)
5. Salloum, S., Gaber, T., Vadera, S., Shaalan, K.: Phishing email detection using natural language processing techniques: a literature survey. Procedia Comput. Sci. **189**, 19–28 (2021)
6. Srihith, I.V.D., Kumar, I.V.S., Varaprasad, R., et al.: Future of smart cities: the role of machine learning and artificial intelligence. South Asian Res. J. Eng. Tech. **4**, 110–119 (2022)
7. Valente, J., Cardenas, A.A.: Understanding security threats in consumer drones through the lens of the discovery quadcopter family. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp 31–36 (2017)

8. Lin, C., He, D., Kumar, N., et al.: Security and privacy for the internet of drones: challenges and solutions. IEEE Commun. Mag. **56**, 64–69 (2018)
9. Liang, C., Miao, M., Ma, J., et al.: Detection of GPS spoofing attack on unmanned aerial vehicle system. In: Chen, X., Huang, X., Zhang, J. (eds.) ML4CS 2019. LNCS, vol. 11806, pp. 123–139. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30619-9_10
10. Dedrone Rolls Out Portable AI-Powered Drone Detection Unit. In: Res. Rep. https://www.verdict.co.uk/de%0Adrone-rolls-out-portable-ai-powered-drone-detection-unit/ (2022). Last Accessed 25 Nov 2022
11. Krajník, T., Vonásek, V., Fišer, D., Faigl, J.: AR-drone as a platform for robotic research and education. In: Obdržálek, D., Gottscheber, A. (eds.) EUROBOT 2011. CCIS, vol. 161, pp. 172–186. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21975-7_16
12. Hooper, M., Tian, Y., Zhou, R., et al.: Securing commercial WiFi-based UAVs from common security attacks. In: MILCOM 2016–2016 IEEE Military Communications Conference, pp. 1213–1218. IEEE (2016)
13. Pleban, J.-S., Band, R., Creutzburg, R.: Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy. In: Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014, pp 168–179. SPIE (2014)
14. Gudla, C,. Rana, M.S., Sung, A.H.: Defense techniques against cyber attacks on unmanned aerial vehicles. In: Proceedings of the International Conference on Embedded Systems, Cyber-Physical Systems, and Applications (ESCS). The Steering Committee of the World Congress in Computer Science, Computer, pp. 110–116 (2018)
15. Astaburuaga, I., Lombardi, A., La Torre, B., et al.: Vulnerability analysis of ar. drone 2.0, an embedded linux system. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 666–672. IEEE (2019)
16. El-Sayed, R., El-Ghamry, A., Gaber, T., Hassanien, A.E.: Zero-day malware classification using deep features with support vector machines. In: 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), pp. 311–317. IEEE (2021)
17. Applebaum, S., Gaber, T., Ahmed, A.: Signature-based and machine-learning-based web application firewalls: a short survey. Procedia Comput. Sci. **189**, 359–367 (2021)
18. Sommer, R., Paxson, V.: Outside the closed world: on using machine learning for network intrusion detection. In: 2010 IEEE symposium on security and privacy, pp. 305–316. IEEE (2010)
19. Abu-Mostafa, Y.S., Magdon-Ismail, M., Lin, H.T.: Learning from Data, vol. 4. New York. NY, USA, AMLBook (2012)
20. Aircrack-ng (2021). Last accessed 25 Nov 2022
21. Hping – active network security tool. In: Hping.org. http://www.hping.org (2021). Last accessed on 25 Nov 2022