algorithms

MDPI

Article

Detection Model for 5G Core PFCP DDoS Attacks Based on Sin-Cos-bIAVOA

Zheng Ma [1], Rui Zhang [1] and Lang Gao [2,*]

[1] Informatization Office, China University of Geosciences, Wuhan 430074, China; mazheng@cug.edu.cn (Z.M.); zhangrui@cug.edu.cn (R.Z.)
[2] Human Resources Department, China University of Geosciences, Wuhan 430074, China
* Correspondence: langgao@cug.edu.cn

Abstract

The development of 5G environments has several advantages, including accelerated data transfer speeds, reduced latency, and improved energy efficiency. Nevertheless, it also increases the risk of severe cybersecurity issues, including a complex and enlarged attack surface, privacy concerns, and security threats to 5G core network functions. A 5G core network DDoS attack detection model is been proposed which utilizes a binary improved non-Bald Eagle optimization algorithm (Sin-Cos-bIAVOA) originally designed for IoT DDoS detection to select effective features for DDoS attacks. This approach employs a novel composite transfer function (Sin-Cos) to enhance exploration. The proposed method's performance is compared with classical algorithms on the 5G Core PFCP DDoS attacks dataset. After rigorous testing across a spectrum of attack scenarios, the proposed detection model exhibits superior performance compared to traditional DDoS detection algorithms. This is a significant finding, as it suggests that the model achieves a higher degree of detection accuracy, meaning it is better equipped to identify and mitigate DDoS attacks. This is particularly noteworthy in the context of 5G core networks, as it offers a novel solution to the problem of DDoS attack detection for this critical infrastructure.

Keywords: 5G; PFCP; cybersecurity; intrusion detection; DDoS

check for updates

Academic Editors: Charalampos Konstantopoulos and Frank Werner

Received: 8 April 2025
Revised: 1 July 2025
Accepted: 17 July 2025
Published: 21 July 2025

Citation: Ma, Z.; Zhang, R.; Gao, L. Detection Model for 5G Core PFCP DDoS Attacks Based on Sin-Cos-bIAVOA. *Algorithms* **2025**, *18*, 449. https://doi.org/10.3390/a18070449

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Fifth-generation (5G) mobile communication technology represents a cutting-edge advancement in mobile systems. It is engineered to provide rapid data transmission speeds, significantly reduced latency, and support for a vast number of simultaneous connections. Today, 5G communication facilities provide the network foundation for realizing the human–machine Internet of Things; 5G technology has a wide range of application scenarios, including enhanced mobile broadband, ultra-high reliability and low-latency communications, and machine-type communications. In addition, 5G technology can provide faster network speeds and lower internal delays, support more device connections, and provide better services for various applications; for example, 5G technology is used in fields such as autonomous driving, telemedicine, and smart homes to improve the performance and reliability of various applications.

The leapfrogging advancements in artificial intelligence, large language models, intelligent agents, and related technologies have introduced new challenges and a range of solutions to modern 5G network security [1]. While the 5G networks bring great convenience to mankind, their security cannot be ignored. The security issues of 5G networks

involve many aspects, including core network, edge network, data security, virtual network technology vulnerability, network business security, network architecture security, encryption security, authentication security, privacy security, and more.

Mobile communication networks [2] can be broadly divided into wireless and core networks, each employing different protocols and interfaces, requiring the application and management of distinct security technologies. Moreover, with multiple sections, security monitoring becomes complicated and traffic analysis to identify security threats is inevitably difficult. The classification of common 5G network security threats is illustrated in Figure 1. In Radio Access Networks (RAN), there are various security threats such as information leaks, user DoS, base-station DoS, eavesdropping, and unauthorized data use. Attackers can exploit paging messages to intercept victims' identities and launch DoS attacks by disrupting connections. They may also attempt to eavesdrop on communications by extracting security keystreams, especially when there are vulnerabilities in the allocation of identifiers. Furthermore, attackers can misuse network bearers for unauthorized purposes such as free data communication or caller spoofing, highlighting the need for robust security measures in RAN to protect user data and service integrity. The 5G core network faces various security threats such as information leakage, IP depletion, DDoS attacks, NAS manipulation, eavesdropping, and IP spoofing, which can impact the network's normal operation and the security of user data.

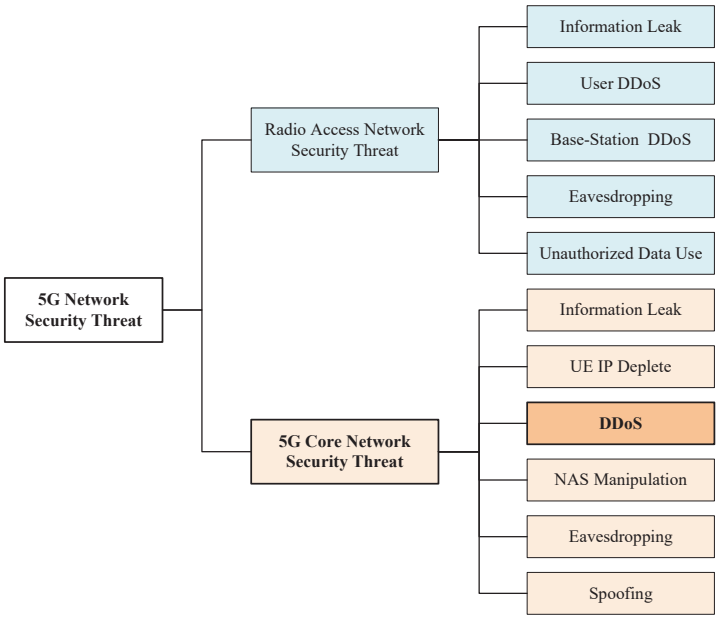


Figure 1. Classification of 5G network security threats. Source: [2].

Given these threats, the security of the 5G core network is crucial [3]. The core network carries user data and business data, and forms the hub of the entire mobile communication network. Today, 5G core networks face a variety of security threats. Major threats include malicious attacks and intrusions, in which hackers can exploit vulnerabilities in the 5G core network to attack and intrude core network elements, obtain sensitive information, disrupt network normality run, etc. Data leakage and privacy invasion are also concerns, as large amount of user data and business data are stored in the 5G core network. If data security protection measures are not in place, data leakage and privacy invasion may occur. Attackers may exploit vulnerabilities in the User-Plane Function (UPF) or Access Management Function (AMF) within the 5G protocol stack by repeatedly initiating attach requests, PDU session establishment requests, and similar signaling, thereby bypassing the legitimate authentication processes of the core network and continuously depleting IP

resources. In a denial of service attack, hackers may launch a denial of service attack on the 5G core network, paralyzing network services or reducing service quality. Attackers can forge legitimate IP addresses to construct malicious packets, exploiting the IP protocol's source address validation flaw to bypass security checks. Additionally, protocol vulnerabilities may be used to alter user plane data, or key reinstallation attacks can be employed to compromise encryption safeguards. Attackers can exploit vulnerabilities in the virtualization management plane, forge session management signaling, and steal user-plane traffic. Spoofing attacks also pose a severe threat to the security of the 5G core network, as attackers may disguise themselves as legitimate users or entities in order to gain unauthorized access, steal sensitive information, or spread malicious software.

The control plane of the 5G Core Network(5GCN) [4] is essential for enabling reliable and high-performance 5G communications by delivering critical services such as authentication, user credential management, and privacy-sensitive signaling. However, the threat landscape has broadened significantly, and the control plane now encounters serious security risks from a variety of sources and interfaces. External network attackers can flood the 5G core network with numerous service requests, overwhelming system resources and impeding legitimate users' access to services. There have not been very many studies investigating the security issues of the 5GCN control plane.

This paper focuses on security issues of the Packet Forwarding Control Protocol (PFCP) utilized in the N4 interface between the Session Management Function (SMF) and the User Plane Function (UPF) in the 5G core network. The study analyzes the characteristics of PFCP DDoS attacks in 5G core networks and explores effective solutions for detecting PFCP DDoS attacks.

The main contributions of this study can be summarized as follows: in Section 2 (Related Work), we conduct an analysis of the PFCP operational mechanisms and the principles of DDoS attacks targeting this protocol; in Section 4 (Experimental Results and Analysis), we propose a Sin-Cos-bIAVOA-based multi-session duration comprehensive analysis PFCP DDoS attack detection model for the PFCP session mechanism; in Section 4.3 (Effectiveness Evaluation Experiment), we utilize publicly available datasets to validate the detection effectiveness of the model in both single-packet DDoS attack scenarios and mixed-packet DDoS attack scenarios; finally, Section 4.4 (Accuracy Comparison Evaluation Experiment) and Section 4.5 (Experiment on the Classification and Identification of Attack Types) describe comparative experiments between our proposed model and traditional machine learning and deep learning methods to evaluate the model's detection accuracy, detection efficiency, and other aspects.

Based on the previous remarks, the rest of this paper is organized as follows: Section 2 introduces the research progress in the field of AI-based DDoS attack detection; Section 3 describes the proposed 5G core PFCP DDoS attack detection method; Section 4 discusses the experimental results and evaluates the method; finally, Section 5 provides the concluding remarks of the paper.

2. Related Work

This section primarily introduces the structure of the 5G core network, working principles of the PFCP protocol, and attack methods, presents the main research directions and progress in the field of attack detection, and describes the experimental environments and datasets proposed by researchers in recent years.

2.1. 5G Core Network DDoS Attacks

The structure of the 5G core network [5,6] is primarily composed of three main components: the access network layer, the transport network layer, and the core network layer.

The access network layer is mainly composed of base stations, and is responsible for the access and management of user equipment (UE) on the wireless side. In 5G, the access network adopts a Centralized Unit (CU) and Distributed Unit (DU) architecture. The CU handles baseband processing such as channel coding and modulation, while the DU is responsible for radio frequency processing such as filtering and power amplification. This architecture optimizes the signal processing process, enhancing network efficiency and performance. The transport network layer [7] consists of a series of operator-owned switching and routing devices, primarily used for transmitting control signaling and user data between the base stations and the core network. The design and implementation of the transport network are crucial for ensuring the efficiency and stability of data transmission. The core network layer deploys a series of core network elements which are responsible for terminal user access and mobility management as well as processing user services. The architecture design and implementation of the core network directly impact the network's availability, reliability, and performance.

As illustrated in Figure 2, the 5G core network architecture [8] comprises the following network functions: Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Network Repository Function (NRF), Policy Control Function (PCF), User Data Management (UDM), Access and Mobility Management Function (AMF), Authentication Server Function (AUSF), Access Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF).

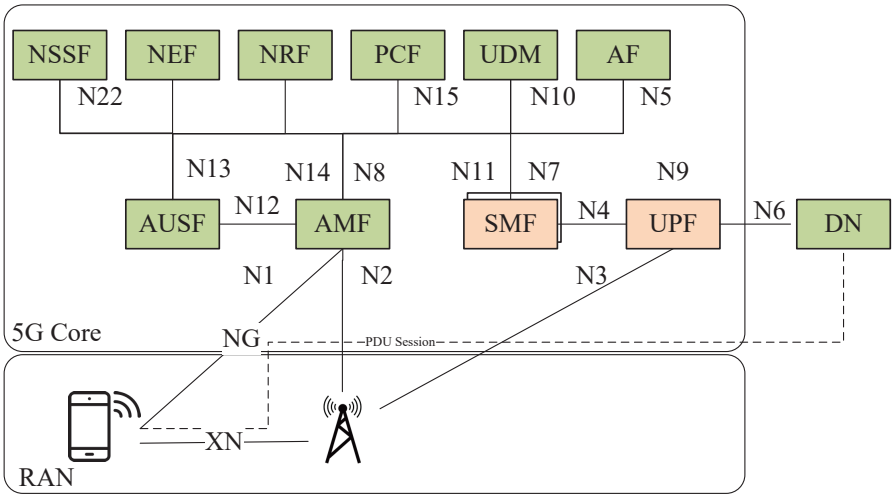


Figure 2. 5G core network structure. Source: [9].

Table 1 illustrates the communication interfaces [10] between various modules in the 5G core network, with the N4 interface serving as the bridge between the UPF and the SMF. The establishment and updating of the N4 interface can be initiated by either the SMF or the UPF; however, the release process is always initiated by the SMF. During the update process, the N4 interface is notified of changes in the network function support characteristics, and the UPF can also use the update process to inform the SMF of resource availability or request that the SMF initiate the release process. Therefore, the N4 interface is particularly noteworthy in the 5G core network and is also a key area for attack prevention.

In this paper, our primary concern revolves around the security challenges associated with the PFCP, a protocol that finds its application in the N4 interface between the SMF and the UPF within the 5G core network.

Table 1. 5G core network interface functions.

Interface	Functions
N1	UE-AMF
N2	gNB-AMF
N3	gNB-UPF
N4	SMF-UPF
N5	PCF-AF
N6	UPF-DN
N7	SMF-PCF
N8	AMF-UDM
N9	UPF-UPF
N10	SMF-PCF
N11	AMF-SMF
N12	AUSF-AMF
N13	AUSF-UDM
N14	AMF-AMF
N15	AMF-PCF
N22	AMF-NSSF

The control plane protocol [11] used for the N4 interface between SMF and UPF is the PFCP protocol, which is defined in the TS 29.244 specification. This protocol is primarily used for SMF to instruct UPF on packet forwarding. The structure of the PFCP message is illustrated in Figure 3. The PFCP consists of a protocol header followed by subsequent Information Elements (IEs). The header contains several key fields, such as the Session Endpoint ID (SEID), MP flag, version, message type, and message length. These fields provide the necessary information and control mechanisms for communication between SMF and UPF. Specifically, the SEID is used to identify and control the amount of subsequent packet content, while the MP flag and version information are used to identify the state and version of the protocol. The message type and message length provide information about the specific content and length of the current message. Together, these pieces of information ensure efficient and accurate communication between the SMF and UPF.

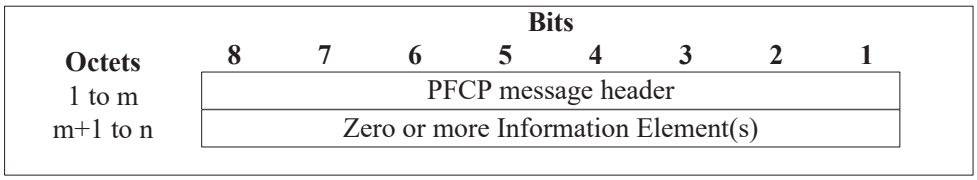


Figure 3. PFCP structure. Source: [12].

The UE sends an NAS registration request [11]. The gNodeB (gNB), which is the base station of the 5G radio access network, receives the registration request from the UE. This request is then forwarded to the AMF, a component within the 5G core network responsible for handling access requests and mobility management. The AMF queries the necessary service information through the NRF, which acts as a service discovery and registration center, aiding the AMF in locating the appropriate services. The AMF sends an authentication request to the AUSF, which is tasked with executing user identity authentication. The AUSF authenticates the UE, which may involve using SIM card information, network authentication tokens, or other authentication mechanisms. If the authentication is successful, the AMF sends a 201 status code to the UE, indicating successful resource creation, and the registration process can proceed. The AMF may need to obtain the URL of the PCF from the NRF for policy control purposes. The AMF interacts with the PCF, which

makes decisions based on the UE's policy requirements, such as QoS rules. The AMF also interacts with the UDM, which is responsible for managing user identities, subscription information, and other data. The SMF is in charge of establishing, modifying, and releasing sessions, working in coordination with the AMF to ensure session continuity. The UPF is responsible for forwarding data to the correct destination. With the completion of the registration process with the 5G network, the UE can now begin using 5G network services.

PFCP is primarily used to establish, modify, and delete sessions between the SMF and UPF [13] as well as to control and manage traffic. The message interaction workflow is illustrated in Figure 4.

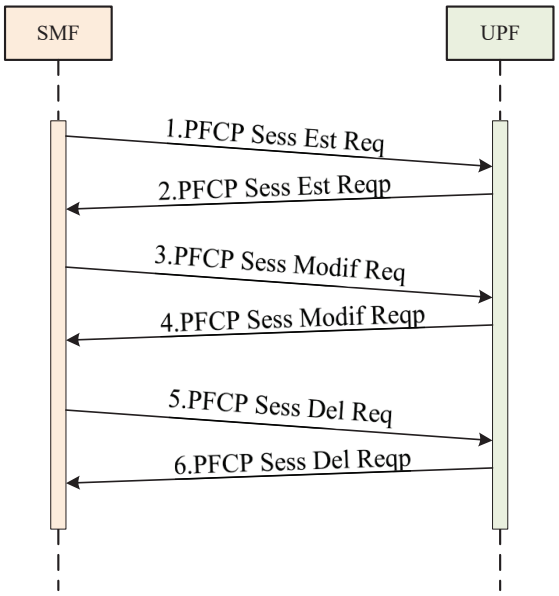


Figure 4. Working principle of PFCP message exchange. Source: [13].

The message interaction workflow includes three sessions. The operational principles and functions of each session are as follows:

- Session establishment: When a UE accesses the 5G network and initiates a service request, the SMF sends a session establishment request to the UPF via PFCP. This request includes session-related parameters such as user identification, service type, and QoS requirements. The UPF creates the corresponding session context based on these parameters and allocates resources to ensure correct transmission of user traffic on the user plane.
- Session modification: During the course of a session, if there is a change in business requirements, such as a user switching from watching a video to engaging in a video call, which entails different QoS requirements for bandwidth and latency, the SMF can send a session modification request to the UPF via the PFCP protocol. The UPF then adjusts resource allocation and traffic handling strategies based on the modified parameters to accommodate the new business requirements.
- Session deletion: When a user terminates a service or when the network side needs to release resources, the SMF sends a session deletion request to the UPF. Upon receiving the request, the UPF releases resources associated with the session, such as closing tunnels and reclaiming bandwidth, thereby completing the session deletion process.

In accordance with the current knowledge related to the PFCP, we can present PFCP exhibits certain network security risks. There are four common types of attacks targeting the PFCP in the core of 5G [14]. These attacks primarily focus on the communication between the SMF and UPF. The four different types of attack principles are as follows:

1. PFCP session establishment DDoS attack: This attack is designed to deplete the UPF's resources by inundating it with numerous legitimate session initiation and heartbeat messages. As a result, the 5G core may be impeded in its capacity to establish new PDU sessions between the client and the DN.
2. PFCP session deletion DDos attack: The goal of this attack is to sever the connection between a particular UE and the DN. It targets the PDU session linking the client to the DN, aiming to disconnect the DN connection while keeping the UE connected to either the NG-RAN or the core network.
3. PFCP session modification flood attack (DROP apply action field flags): The goal of this attack is to disable the packet processing rules associated with a specific session, ultimately causing the target UE to disconnect from the DN.
4. PFCP session modification flood attack (DUPL apply action field flag): This attack is designed to take advantage of the DUPL flag within the application action field, compelling the UPF to replicate session rules, thereby creating several pathways for data originating from a single source.

2.2. 5G Core Network DDoS Attack Detection Methods

In 5G core networks, DDoS attacks are a common attack method that cause network paralysis or failure to operate properly by occupying a large amount of network resources. In order to detect DDoS attacks, several methods can be adopted. Over the past two years, trends in DDoS attacks have led researchers to analyze several mitigation strategies based on software-defined networking (SDN), network function virtualization (NFV), and mobile target defense [15], while emphasizing several challenges encountered when employing innovative technologies to counteract DDoS attacks. Onoja [16] and colleagues introduced a security approach for 5G networks that mitigates DDoS attacks by actively managing threat responses. Their method utilizes a reactive, event-focused security policy language, fostering a flexible, efficient, and lightweight defense strategy. Mamolar, A.S. et al. [17] introduced an innovative method to address the shortcomings of conventional detection systems. They developed a new sensor that can collect the necessary data to trace an attacker even if the attacker is moving across multiple locations. Furthermore, the authors of [18] proposed an autonomous security system—comprising its design, implementation, and empirical validation—that effectively shields networks from Distributed Denial of Service (DDoS) attacks by autonomously selecting and executing appropriate countermeasures without human intervention. Ramezan, G. [19] and colleagues introduced an extensible authentication protocol called EAP-ZKP which is applicable in both initial and subsequent authentication stages to help mitigate DDoS attacks along the CN edge. A novel defense framework [20] integrates real-time threat detection with proactive mitigation to neutralize signaling-based DDoS attacks in 5G standalone core networks. Some researchers used a novel [21] enhanced naive Bayes algorithm. This method not only examines both the independent and interdependent aspects of features through structural improvements but also employs a genetic algorithm to identify the optimal combination of attribute weights for effective categorization. A hybrid classification framework for 5G DDoS attacks combining deep neural networks with a modified equilibrium optimization algorithm (MEOADL-ADC) was proposed in [22], achieving superior detection accuracy through adaptive feature learning and parameter optimization. Based on an actor–critic reinforcement learning framework [23], Slice Isolation-Based Reinforcement Learning (SIRL) mitigates DDoS attacks in Beyond-5G networks by dynamically configuring a graph-based environment. The model leverages five optimized graph features to represent network states and employs a ranking-driven adjustment mechanism to adapt its defense strategy in real time, enhancing resilience against evolving attack patterns. The deep learning frame-

work in [24,25] detects DDoS attacks in 5G slices and deploys a resource-minimal sinkhole slice to isolate malicious traffic, which was validated in a 5G prototype for autonomous attack containment. The DDoS intrusion detection framework in [26] was designed for dynamic IoT environments, effectively counteracting one of the top threats to data flow in IoT networks. Their approach utilizes a Kalman backpropagation neural network to enhance the detection and mitigation of DDoS attacks. The federated-learning framework in [27] enables privacy-preserving DDoS detection on the GTP protocol in 5G core networks by aggregating distributed device intelligence for real-time attack identification. This approach eliminates centralized data sharing while maintaining detection accuracy through collaborative model training across network nodes. Fang, L.M. [28] and colleagues proposed a countermeasure against DDoS attacks in the 5G context by integrating smart contracts with machine learning. Their approach conceals a secure server within a blockchain network and dynamically controls the scale of attacks through adjustments in transaction fees. A randomized backward learning enhancement to the African Vultures Optimization Algorithm (AVOA) yielded the IA-VOA variant [29], demonstrating superior convergence speed, stability, and reliability across experimental benchmarks. Finally, the AVO-DT metaheuristic decision tree framework [30] integrates the AVOA to enhance malware detection accuracy by optimizing tree construction through global search and local exploitation.

In summary, biomimetic intelligent optimization algorithms hold vast potential for application in DDoS attack detection. These algorithms can handle high-dimensional data, address issues with data noise, and compensate for the shortcomings of traditional approaches. By utilizing biomimetic intelligent optimization algorithm, it is possible to learn and extract features from network traffic data. These features can be used to classify normal and attack traffic, making it possible to detect DDoS attacks. In practical applications, suitable biomimetic intelligent optimization algorithms can be selected based on specific circumstances, or multiple methods can be combined for comprehensive detection. Timely identification and handling of security incidents are crucial to ensuring the secure and reliable operation of 5G core networks.

2.3. Relevant Intrusion Detection Datasets for Security Testing and Malware Prevention

It is evident that intrusion detection mechanisms empowered with Artificial Intelligence (AI) models play a crucial role. To further investigate the characteristics of 5G networks, and in particular to evaluate the attack detection capabilities and effectiveness of AI models, researchers have conducted relevant studies focusing on 5G experimental platforms and datasets. The Vulnerability Assessment Approach (VAA) [31] is used to identify and evaluate vulnerabilities in 5G networks, particularly focusing on 5G Edge networks. The VAA utilizes the TOPSIS technique to analyze vulnerabilities from an attacker's perspective, considering the dynamic and scalable nature of 5G Edge networks. G. Amponis [32] led a team in designing a labeled security dataset named the "5GC PFCP Intrusion Detection Dataset" as part of a cloud-based 5G Edge security testbed introduced to evaluate the VAA's accuracy, scalability, and performance. The dataset comprises network flow analytics designed for AI detection models to identify cyberattacks aimed at the Packet Forwarding Control Protocol (PFCP) utilized in the N4 interface of 5G core systems. It examines four distinct PFCP attack scenarios, offering crucial network traffic data through pcap files as well as detailed TCP/IP and application-layer metrics. The dataset consists of balanced TCP/IP and PFCP flow statistics, with an equal number of samples for each class, facilitating the training and testing of machine learning and deep learning algorithms for intrusion detection. They also proposed a containerized 5G testbed [33] designed to train defenders and develop intrusion detection systems by emulating various network functions and implementing specific attack scenarios, including full-stack attacks

targeting both networked hosts and 5G network functions. The testbed generates malicious datasets containing traffic from both classical and 5G-specific attacks, which can be used to train AI and ML systems for proactive threat detection. J. Ock et al. [34] explored the use of synthetic data generation for anomaly detection in the 5G NWDAF architecture. Due to the challenges of insufficient training data quality and quantity in NWDAF, they proposed using CTGAN to generate high-quality synthetic 5G NWDAF data. They then conducted experiments and evaluate the quality of the synthetic data and the resulting anomaly detection performance, finding that CTGAN-generated synthetic data can be a promising alternative to address data scarcity issues. Researchers have also utilized the NIDS datasets in [35] as a network testing platform to create synthetic datasets for public research. These datasets comprise labeled network flows constructed from features extracted from network traffic. 5G-NIDD [36] is a fully annotated dataset constructed on a fully functional 5G test network, and is available for researchers developing and testing AI/ML solutions. The test platform for the WUSTL-HDRL-2024 dataset [37] is designed to simulate a dynamic 5G network environment. This dataset meets the need to comprehensively capture various interactions and security threats within 5G networks. Moubayed, A. [38] proposed a framework design that integrates Exploratory Data Analysis (EDA) and Deep Learning (DL) for 5G network intrusion detection. Tests using the 5G-NIDD dataset demonstrated that the method possesses exceptional capabilities in both intrusion detection and attack identification. Researchers have employed various sampling methods to balance benign and malicious traffic in 5G networks; however, they often overlook the imbalance among different types of malicious traffic. CoSen-IDS [39] addresses this imbalance issue through cost-sensitive learning. The NetsLab-5GORAN-IDD dataset [40] integrates both higher-layer network packet data and lower-layer radio telemetry, offering a comprehensive view of normal and malicious activity within a realistic 5G O-RAN deployment. Captured during controlled attack scenarios, the dataset includes benign traffic as well as multiple types of network-layer attacks targeting the O-Cloud Edge Server.

3. Method

In this section, the principle of the AVOA algorithm and its optimization method based on sin-cos are introduced, with a focus on presenting the proposed PFCP DDoS attack detection model based on this algorithm.

3.1. AVOA

The AVOA algorithm is a swarm intelligence optimization algorithm that simulates the foraging behavior of African Vultures for global optimization. In 2021, Benyamin Abdollahzadeh et al. [41] proposed this algorithm, which performs optimization by mimicking the leader–follower model and natural predation behavior of African Vultures.

As shown in Figure 5, the principles of the AVOA algorithm mainly include the following stages:

1. Population Initialization: A certain number of individuals are randomly generated as the initial population.
2. Fitness Evaluation: The fitness value of each individual is calculated based on the problem's fitness function.
3. Selection Operation: Individuals are sorted according to their fitness values; those with higher fitness are selected as elite individuals to be retained for the next generation.
4. Behavior Simulation: Includes two phases, blind search and local search; in blind search, individuals move randomly by a certain distance in the hope of finding better solutions, while in local search individuals search around the current best solution to find solutions closer to the optimal solution.

5. Population Update: The population is updated based on the new positions.
6. Termination Condition Check: It is determined whether the termination condition is met. If so, the algorithm ends; otherwise, it returns to step 3.

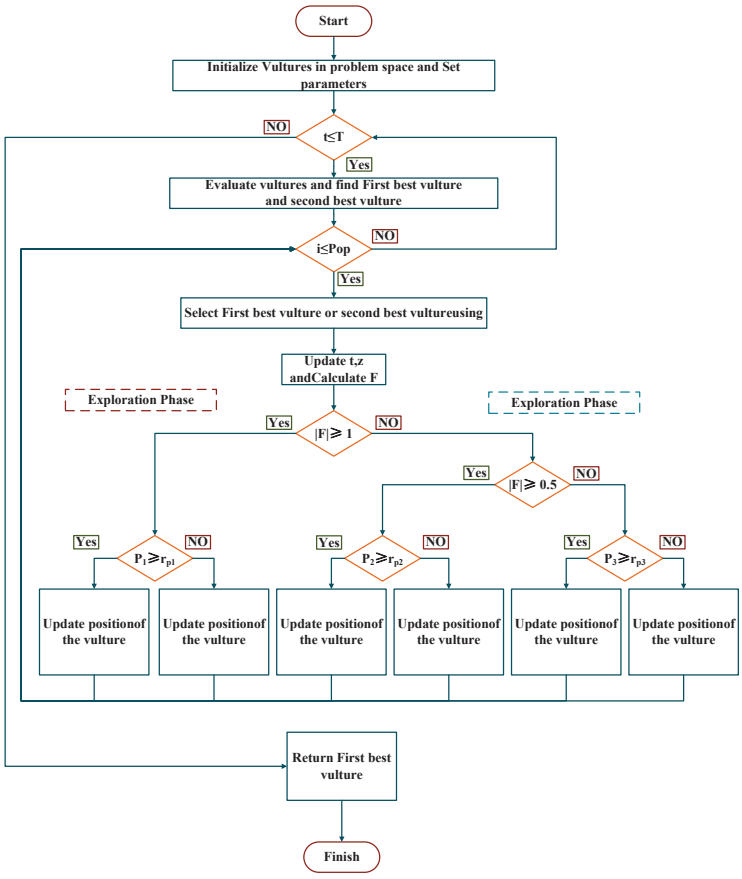


Figure 5. Flowchart of AVOA.

The mathematical model of the AVOA algorithm consists of four main components: leader selection, vulture hunger rate, exploration phase, and exploitation phase. Leader selection is determined by calculating the fitness of all solutions to choose the optimal one as the leader. The hunger rate acts as a conversion factor, determining whether the vultures will search for food at greater distances or forage around the strongest solution. The exploration and exploitation phases employ different strategies based on the vulture hunger rate and current position, aiming to find the global optimal solution. The AVOA algorithm is characterized by its strong optimization capability and rapid convergence speed. It has been applied in numerous practical engineering projects and has demonstrated its superiority through tests on 36 standard benchmark functions.

3.2. Sin-Cos-bIAVOA

AVOA suffers from the drawbacks of slow convergence speed and local optimum stagnation. In response to various complex optimization tasks and different application scenarios, researchers have proposed several enhanced optimization methods based on AVOA, tailored to the specific requirements [42–44]. Zakieh Sharifian et al. [45] introduced an enhanced binary version of AVOA termed Sin-Cos-bIAVOA, designed for selecting effective features pertinent to DDoS attacks. This approach incorporates an innovative compound sin-cos transfer function to boost exploratory capabilities while employing the Gravitational Fixed Radius Nearest Neighbor (GFRNN) classifier for identifying the optimal feature subset.

Sin-Cos-bIAVOA operates through three distinct phases. Initially, the algorithm probes new and promising regions to prevent premature convergence and avoid local optima. In the subsequent phase, it gradually transitions from exploration to exploitation. Finally, the algorithm focuses on fine-tuning around the highest-quality solutions to identify the optimal outcome. Figure 6 illustrates the detailed steps and overall workflow of the algorithm. After the population is initialized, the sin-cos transfer function is employed to generate binary positions. In this algorithm, the input parameters include the population (N), dimension (D), and maximum number of iterations. The number of vultures in an environment is simulated as the population (N), while D is the dimension of the problem. The output parameters are the optimal and suboptimal results.

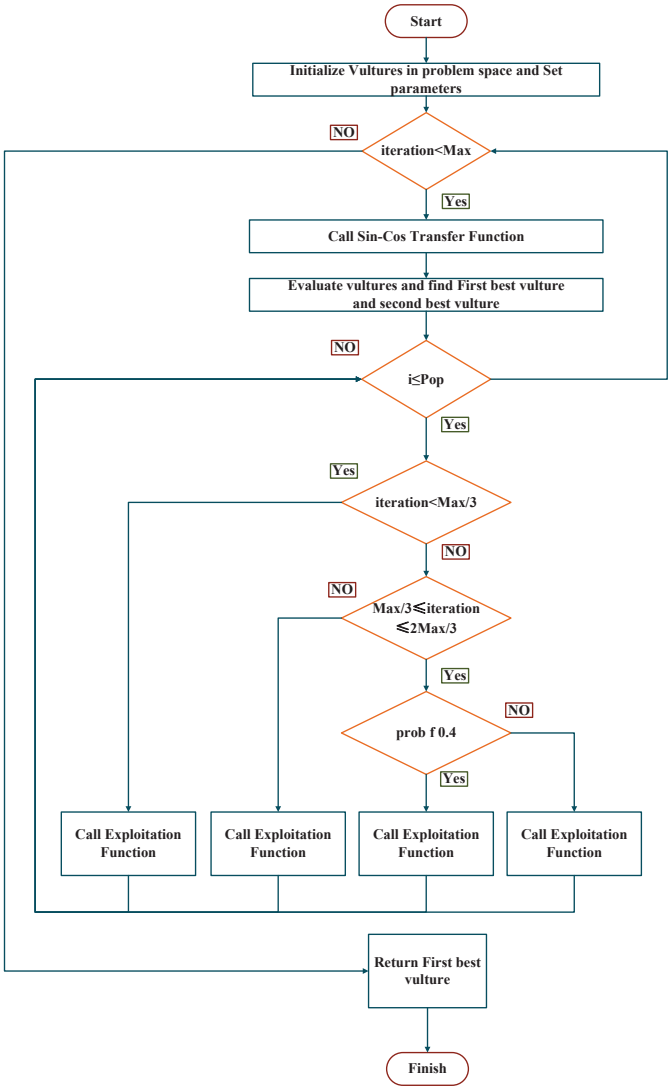


Figure 6. Workflow of Sin-Cos-bIAVOA.

A new compound transfer function, termed sin-cos, is introduced to convert continuous representations into binary ones. This function enhances the exploration capabilities of bIAVOA by generating a highly diverse population. It operates by applying a specific set of functions and rules [45] to map the continuous search space into its binary equivalent:

$$S_1(x_{ij}) = Cos(x_{ij})/2 + 0.5 \quad (1)$$

$$x'_{ij} = \begin{cases} 1 & if\, rand_1() < S_1(x_{ij}) \\ 0 & if\, rand_1() \geq S_1(x_{ij}) \end{cases} \quad (2)$$

$$S_2(x_{ij}) = Sin(x_{ij})/2 + 0.5 \quad (3)$$

$$x''_{ij} = \begin{cases} 1 & if\, rand_2() < S_2(x_{ij}) \\ 0 & if\, rand_2() \geq S_2(x_{ij}) \end{cases} \quad (4)$$

$$x_i = \begin{cases} x'_i & if\, f(x'_i) is\, better\, than f(x''_i) \\ x''_i & if\, f(x''_i) is\, better\, than f(x'_i) \end{cases} \quad (5)$$

where x_{ij} is the current continuous position of the ith vulture in the jth dimension and f(.) is the fitness function. Sin(.) and Cos(.) are sine and cosine functions, respectively; the functions Sin(.) and Cos(.) generate two values in the range of [0, 1], and two new binary positions are created according to Equations (1) and (3). The position with the highest fitness value is chosen and labeled as x_i, representing its new location in the binary search space. The two functions Sin(.) and Cos(.) along with these rules generate a diverse range of solutions and enhance the algorithm's ability to explore new possibilities. The pseudocode for the sin-cos transfer function is provided in Figure 7.

Pseudocode of Sin-Cos Transfer Function

Function Sin-Cos
Inputs: Viltures' postions(x), dimension
1. ***for*** *j=1* to *dimension* **do**
2. $S_1(x_{ij}) = Cos(x_{ij})/2 + 0.5$
3. **if** $S_1(x_{ij})$ **p** $rand_1()$ **then**
4. $x'_{ij} = 1$
5. **else**
6. $x'_{ij} = 0$
7. $S_2(x_{ij}) = Sin(x_{ij})/2 + 0.5$
8. **if** $S_2(x_{ij})$ p $rand_2()$ **then**
9. $x''_{ij} = 1$
10. **else**
11. $x''_{ij} = 0$
12. Compute Fitness value $x'_i : f(x'_i)$
13. Compute Fitness value $x''_i : f(x''_i)$
14. **if** $f(x'_i)$ **is better than** $f(x''_i)$
15. $x_i = x'_i$
16. $f(x_i) = f(x'_i)$
17. **else**
18. $x_i = x''_i$
19. $f(x_i) = f(x''_i)$
20. **End**
21. **return** x_i, $f(x_i)$

Figure 7. Sin-Cos transfer function.

3.3. PFCP DDoS Attack Detection Model

DDoS attack detection is part of the Detect functionality within the Core category of the NIST Cybersecurity Framework. Specifically, this function aims to identify potential cybersecurity incidents through continuous monitoring and anomaly analysis, with DDoS attack detection serving as a key technology for recognizing abnormal traffic or malicious behavior.The control plane of the 5G core network adopts a service-based architecture design. In this service-based architecture, network elements are connected to the same

line, each with a service-based interface that allows them to interact with other network elements externally. As illustrated in Figure 8, the 5G network is a packet-switched network, in which the concepts of the control plane and the user plane have always existed. The control plane and user plane are categorized based on the type of data they handle; the control plane is responsible for transmitting control signaling (signaling interaction), while the user plane is responsible for transmitting actual data.

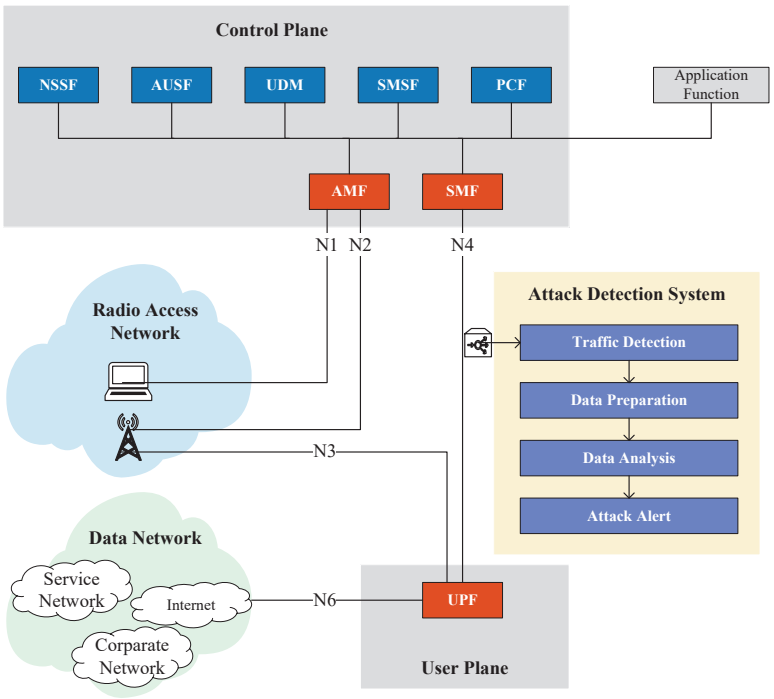


Figure 8. Network structure of the 5G core PFCP DDoS attack detection model.

Taking the N4 interface as an example, this paper considers the potential risks in the communication process between the UPF and the SMF. First, the UPF communicates directly with the operator's data network, and its ports may be exposed to the public network; additionally, due to the separation of control plane and user plane in the 5GC architecture, the UPF needs to be deployed at the network edge, increasing the risk of exposure. The establishment process of the N4 interface is initiated by the SMF and sent to the UPF. If the UPF lacks a robust authentication mechanism for network elements, attackers could impersonate the SMF to launch attacks on the UPF. The PFCP protocol supports several business processes, including session establishment, session modification, session deletion, and session reporting. After establishing a connection with the UPF using a forged SMF, attackers can exploit the session modification process to redirect user plane data packets for data theft or can use the session deletion process to deny service to certain users.

DDoS attacks on the 5G core network occur primarily between the SMF and UPF units. Therefore, deploying traffic collection probes at the N4 interface to collect and analyze network traffic on the N4 interface can most effectively enable DDoS attack detection and early warning.

The entire traffic detection system comprises four main components: traffic collection, data preprocessing, data analysis, and attack alerting. Among these, data preprocessing and data analysis are the most critical, with their algorithmic principles and models illustrated in Figure 9.

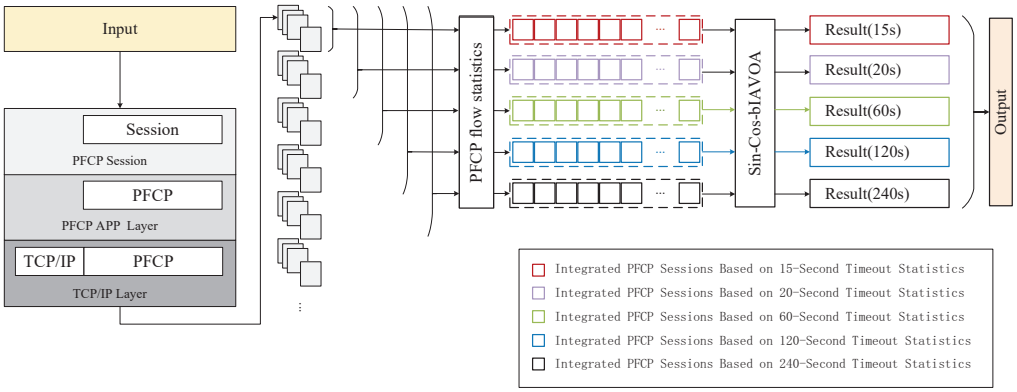


Figure 9. Principle of the 5G core PFCP DDoS attack detection model.

The detection model obtains raw traffic data from the traffic probe. Traffic packets are parsed according to the TCP/IP protocol format, with layered parsing of network layer TCP/IP protocol data and application layer PFCP protocol data, and feature values are extracted to form a dataset. Based on different timeout durations (15 s, 20 s, 60 s, 120 s, 240 s), PFCP protocol sessions are statistically integrated. Session data are detected using the Sin-Cos-bIAVOA algorithm. Finally, the detection results are summarized and comprehensively analyzed to generate DDoS alert information for output. The attack detection model captures network data through the N4 interface and accurately identifies both attack packets and attack sessions by analyzing multiple timeout dimensions, enabling the detection of PFCP DDoS attacks in the 5G core network. This model represents an innovative practical application of the Sin-Cos-bIAVOA algorithm, achieving attack detection through a comprehensive process that encompasses data collection, data integration, and data analysis and processing.

4. Experimental Results and Analysis

In this section, the model is evaluated using publicly available datasets. Its effectiveness in detecting both single-type and mixed-type attacks is tested, its performance is compared with other algorithms, and its recognition accuracy for various attack types is further assessed.

4.1. Experimental Environment and Equipment Configuration

The experiment was conducted on a workstation equipped with an NVIDIA GeForce RTX 3060 graphics card and an Intel Core i7 processor. This hardware configuration provides sufficient performance for graphical processing and deep learning computational requirements. The software environment utilized the Windows 11 operating system. Algorithm implementation employed the MATLAB R2024a programming language, utilizing both the Deep Learning Toolbox and the Statistics and Machine Learning Toolbox.

4.2. Experimental Dataset

George Amponis et al. [32] introduced the 5G Core PFCP Intrusion Detection Dataset. This resource comprises a collection of network flow statistics designed for AI-based detection models to identify cyberattacks aimed at the PFCP. PFCP facilitates communication on the N4 interface between the SMF and the UPF within the 5G core. The public datasets have been released by IEEE Dataport.

This dataset contains network traffic and traffic statistics for each entity involved. Specifically, each 7z/zip file includes the following: pcap files, TCP/IP network traffic

statistics, PFCP flow statistics, and statistics using different timeout values (e.g., 15, 20, 60, 120, and 240 s).

Based on the previous remarks, the dataset was divided into six distinct sub-datasets: PFCP Session Deletion DoS Attack, PFCP Session Establishment DoS Attack, two variants of PFCP Session Modification DoS Attack (DROP and DUPL), Balanced PFCP APP Layer, and Balanced TCP-IP Layer. For training and testing, the data were split at a ratio of 70% to 30%, respectively, with a stratified approach ensuring that each subset contained the same class proportions.

4.3. Effectiveness Evaluation Experiment

To assess the performance of the proposed method, this study utilizes a range of metrics, including accuracy, precision, recall, F-measure, specificity, and Feature Reduction Rate (FRR), as defined below.

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$F\text{-}measure = 2 \times \frac{Precision \times recall}{Precision + recall} \tag{9}$$

$$Feature\ Reduction\ Rate = \frac{Number\ of\ Reduction\ Feature}{Total\ Features} \tag{10}$$

In this context, TP denotes the count of DDoS attack records that have been accurately identified and TN represents the number of normal records that were correctly classified; conversely, FN and FP correspond to misclassified DDoS attack and normal records, respectively.

The results of the algorithms on the datasets are provided in Tables 2–5. The tables present the detection results for the Deletion DDoS Attack, Establishment DDoS Attack, Modification DDoS Attack DROP, and Modification DDoS Attack DUPL datasets, which represent four distinct types of single-attack traffic. Each set of experimental data includes normal traffic and a single type of attack. The proposed algorithm demonstrates high detection accuracy across all five session scenarios with varying timeouts (15 s, 20 s, 60 s, 120 s, and 240 s).

The experimental results demonstrate the proposed algorithm's comprehensive performance in detecting PFCP DDoS attacks against the 5G core network. By focusing particularly on the Deletion DDoS Attack, Establishment DDoS Attack, Modification DDoS Attack DROP, and Modification DDoS Attack DUPL datasets, each of which represents a unique type of single-attack traffic, the results provide an in-depth analysis of the algorithm's capabilities in identifying these distinct forms of cyber intrusions. Notably, the algorithm consistently demonstrated high detection accuracy across all five session scenarios, each with varying timeouts (15 s, 20 s, 60 s, 120 s, and 240 s). This array of timeout settings allows for a broad evaluation of the algorithm's performance under different conditions of urgency and computational load, further highlighting its robustness and efficiency in identifying cyber threats in real-time scenarios.

Table 2. Results on PFCP session deletion DDos attack dataset.

Timeout (s)	Fitness	Feature Reduction Rate	Accuracy (%)	Precision(%)	Recall (%)	Specificity (%)	F-Measure (%)
15	0.011232	0.050633	98.9166	98.4646	100	96.4506	99.2264
20	0.010144	0.037975	99.0137	98.547	99.9133	97.4665	99.2255
60	0.011539	0.037975	98.8728	98.25	100	96.9298	99.1173
120	0.009363	0.025316	99.0798	98.5294	100	97.6	99.2593
240	0.004965	0.050633	99.5495	99.359	100	98.5075	99.6785

Table 3. Results on PFCP session establishment DDoS attack dataset.

Timeout (s)	Fitness	Feature Reduction Rate	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F-Measure (%)
15	0.002626	0.012658	99.7475	100	99.5816	100	99.7904
20	0.002590	0.025316	99.7639	100	99.6109	100	99.8051
60	0.008907	0.025316	99.1259	100	98.5994	100	99.2948
120	0.000253	0.025316	100	100	100	100	100
240	0.000253	0.025316	100	100	100	100	100

Table 4. Results on PFCP session modification DDoS attack DROP dataset.

Timeout (s)	Fitness	Feature Reduction Rate	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F-Measure (%)
15	0.000795	0.025316	99.9452	100	99.9155	100	99.9577
20	0.002002	0.075949	99.8745	99.8917	99.8917	99.8507	99.8917
60	0.002100	0.025316	99.8134	100	99.6732	100	99.8363
120	0.000253	0.025316	100	100	100	100	100
240	0.000253	0.025316	100	100	100	100	100

Table 5. Results on PFCP session modification DDoS attack DUPL dataset.

Timeout (s)	Fitness	Feature Reduction Rate	Accuracy (%)	Precision (%)	Recall(%)	Specificity (%)	F-Measure (%)
15	0.001448	0.10127	99.9559	99.9393	100	99.8397	99.9696
20	0.000253	0.025316	100	100	100	100	100
60	0.000253	0.025316	100	100	100	100	100
120	0.000253	0.025316	100	100	100	100	100
240	0.000126	0.012658	100	100	100	100	100

4.4. Accuracy Comparison Evaluation Experiment

This section aims to evaluate the detection performance of various algorithms in terms of their DDoS attack detection by comparing their effectiveness under different timeout values. The goal is to determine the adaptability of different algorithms in detecting attacks within various time windows (timeout values), thereby providing theoretical support and practical guidance for DDoS attack detection in real applications. The experimental dataset utilizes a mixed dataset in which attack packets and normal packets are proportionally balanced at a ratio of 1:1. To increase the complexity of the experiment and further assess the accuracy and adaptability of the algorithms, the attack packets are evenly distributed among four types of attacks: PFCP session establishment DDoS attack, PFCP session deletion DDoS attack, PFCP session modification flood attack (DROP apply action field flag), and PFCP session modification flood attack (DUPL apply action field flag). The experiment introduces eight commonly used attack detection algorithms for comparison: Back-Propagation (BP), Convolutional Neural Network (CNN), Radial Basis Function

(RBF), Extreme Learning Machine (ELM), Random Forest (RF), Support Vector Machine (SVM), Long Short-Term Memory (LSTM), and AVOA.

The experiment also established five different timeout values (15 s, 20 s, 60 s, 120 s, and 240 s) to simulate the detection performance under different time windows. The selection of timeout values aims to cover detection scenarios from short time windows to long time windows. The experimental results are shown in Table 6, with detection accuracy as the main performance metric used to evaluate the effectiveness of each algorithm under different timeout values.

Table 6. Results on balanced PFCP session DDos attack dataset.

Timeout (s)	15 s	20 s	60 s	120 s	240 s	Average
Sin-Cos-bIAVOA	0.9821	0.9769	0.9740	0.9749	0.9895	0.97948
AVOA	0.9168	0.9326	0.9391	0.9452	0.9079	0.92832
BP	0.9737	0.9760	0.9365	0.9713	0.9685	0.9652
CNN	0.9770	0.9692	0.9452	0.9427	0.9755	0.96192
RBF	0.9287	0.9342	0.9240	0.9229	0.9406	0.93008
ELM	0.9455	0.9345	0.9317	0.9337	0.9336	0.9358
RF	0.9786	0.9711	0.9711	0.9606	0.9720	0.97068
SVM	0.9488	0.9378	0.9308	0.9337	0.9231	0.93484
LSTM	0.9494	0.9313	0.9423	0.9444	0.9650	0.94648

Figure 10 provides a visual comparison of the detection accuracy results for various algorithms under different timeout values. The Sin-Cos-bIAVOA algorithm consistently exhibits the highest detection accuracy across all timeout values, with an average accuracy of 0.97948. This indicates that the algorithm demonstrates high robustness and adaptability in detecting DDoS attacks. Additionally, most algorithms achieve high detection accuracy under short timeout values (15 s, 20 s), likely due to the ease of capturing traffic characteristics within short time windows. However, the performance of some algorithms declines in longer timeout values (120 s, 240 s), possibly due to the interference caused by data noise over extended time windows. The AVOA algorithm optimized using the sin-cos method demonstrates a higher detection accuracy compared to the original method. The Sin-Cos-bIAVOA algorithm maintains a high level of performance even at longer timeout values, demonstrating its strong capability in handling complex traffic patterns.

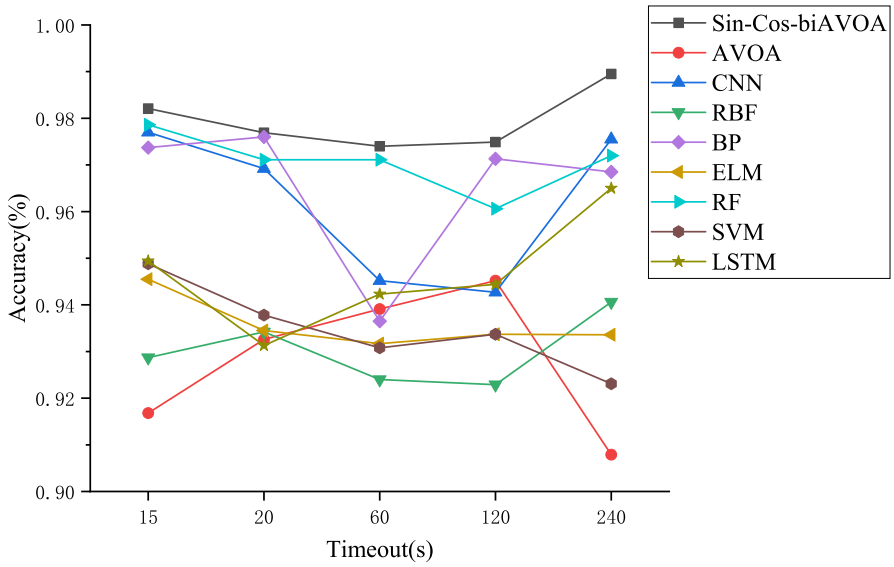


Figure 10. Results on balanced PFCP session DDos attack dataset.

4.5. Experiment on Classification and Identification of Attack Types

In the previous section, the comparative experimental results demonstrated that the proposed method achieves higher detection accuracy relative to traditional machine learning algorithms for binary classification applications such as attack detection, confirming its ability to effectively identify PFCP DDOS attack traffic in 5G core networks. Building on this, another experiment was designed to further validate the algorithm's recognition accuracy across different attack types.

The experimental dataset in this subsection employs a mixed dataset in which attack packets and normal packets are balanced in a 4:1 ratio. The attack packets are evenly distributed among four types of attacks: PFCP session establishment DDoS attacks, PFCP session deletion DDoS attacks, PFCP session modification flooding (DROP) attacks, and PFCP session change flooding (DUPL) attacks. In the mixed dataset, the packet counts for the five categories are approximately evenly distributed. Each category is assigned a distinct timeout (15 s, 20 s, 60 s, 120 s, and 240 s, respectively) in order to increase the complexity of the experiment and allow for further evaluation of the the proposed algorithm's accuracy and adaptability.

The experimental results are shown in Table 7. The accuracy for the five different timeouts ranging from 15 s to 240 s is 81.713%, 79.4907%, 84.478%, 86.445%, and 89.5522%, respectively, showing an initial slight decline followed by a gradual increase. The highest accuracy of 89.5522% is achieved with the longest timeout of 240 s. A comprehensive analysis of the various metrics indicates that with an adequate extension of the timeout period, the proposed attack detection classification algorithm demonstrates a notable performance improvement in several aspects, including feature reduction, accuracy, precision, recall, specificity, and F-value. Notably, all of these metrics reach relatively high levels when the timeout is set to 240 s.

Table 7. Results of the classification and identification of attack types experiment.

Timeout(s)	Fitness	Feature Reduction Rate	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F-Measure (%)
15	0.18319	0.21519	81.713	81.7937	81.5645	95.4375	81.6789
20	0.20431	0.12658	79.4907	79.4623	78.833	94.8953	79.1464
60	0.15835	0.46835	84.478	83.7885	84.0444	96.1426	83.9162
120	0.1404	0.62025	86.445	86.7326	86.1504	96.6255	86.4405
240	0.10824	0.48101	89.5522	90.3047	89.5645	97.4019	89.9331

To comprehensively evaluate the performance of the classification algorithm, a 5×5 confusion matrix is employed in Figure 11 to visually display the distribution of the classification results. The results reveal the algorithm's recognition ability for different classes, clearly illustrating the prediction confusions for each class. The experiment conducted classification tests on five types of communication packets, with the specific labels being as follows: 1, normal data; 2, establishment DDoS attack; 3, deletion DDoS attack; 4, modification DDoS (DROP) attack; 5, modification DDoS (DUPL) attack. The classification performance of the algorithm was also evaluated under five distinct timeout conditions.

A comparison of the confusion matrix results under different timeout conditions reveals that the timeout duration has a significant impact on the performance of the classification algorithm. The values along the main diagonals demonstrate that the overall classification accuracy varies under different timeout conditions. With extended timeout durations, a certain level of classification accuracy can be maintained. In terms of categorization, the algorithm is more accurate for the normal data, establishment DDoS attack, and deletion DDoS attack data types, while the accuracy for the modification DDoS (DROP) attack and modification DDoS (DUPL) attack data types is slightly lower.

4.6. Discussion

The experimental results verify the superiority of the proposed Sin-Cos-bIAVOA algorithm in detecting 5G PFCP DDoS attacks. Comparing the detection performance of various algorithms under different timeout values, the results indicate that the proposed algorithm maintains high detection accuracy in both short-term and long-term windows, demonstrating strong robustness and adaptability.

In binary classification attack detection, the proposed algorithm exhibits high detection accuracy for four types of single-category attack traffic, particularly excelling when the timeout is set to 240 s. In the experiment on balanced traffic attack detection conducted over time intervals ranging from 15 to 240 s, the proposed algorithm outperforms other commonly used machine learning and deep learning algorithms, achieving an average accuracy of 97.948%.

In multi-class attack detection, the proposed attack detection algorithm demonstrates a consistent trend of performance improvements across multiple metrics as the timeout is appropriately extended, with all indicators reaching high levels when the timeout is 240 s.

The model still has room for further optimization, particularly in terms of detection accuracy on balanced datasets. Moreover, the model needs to be further adapted to the higher demand for attack detection efficiency in the high-concurrency and high-traffic scenarios typical of 5G networks.

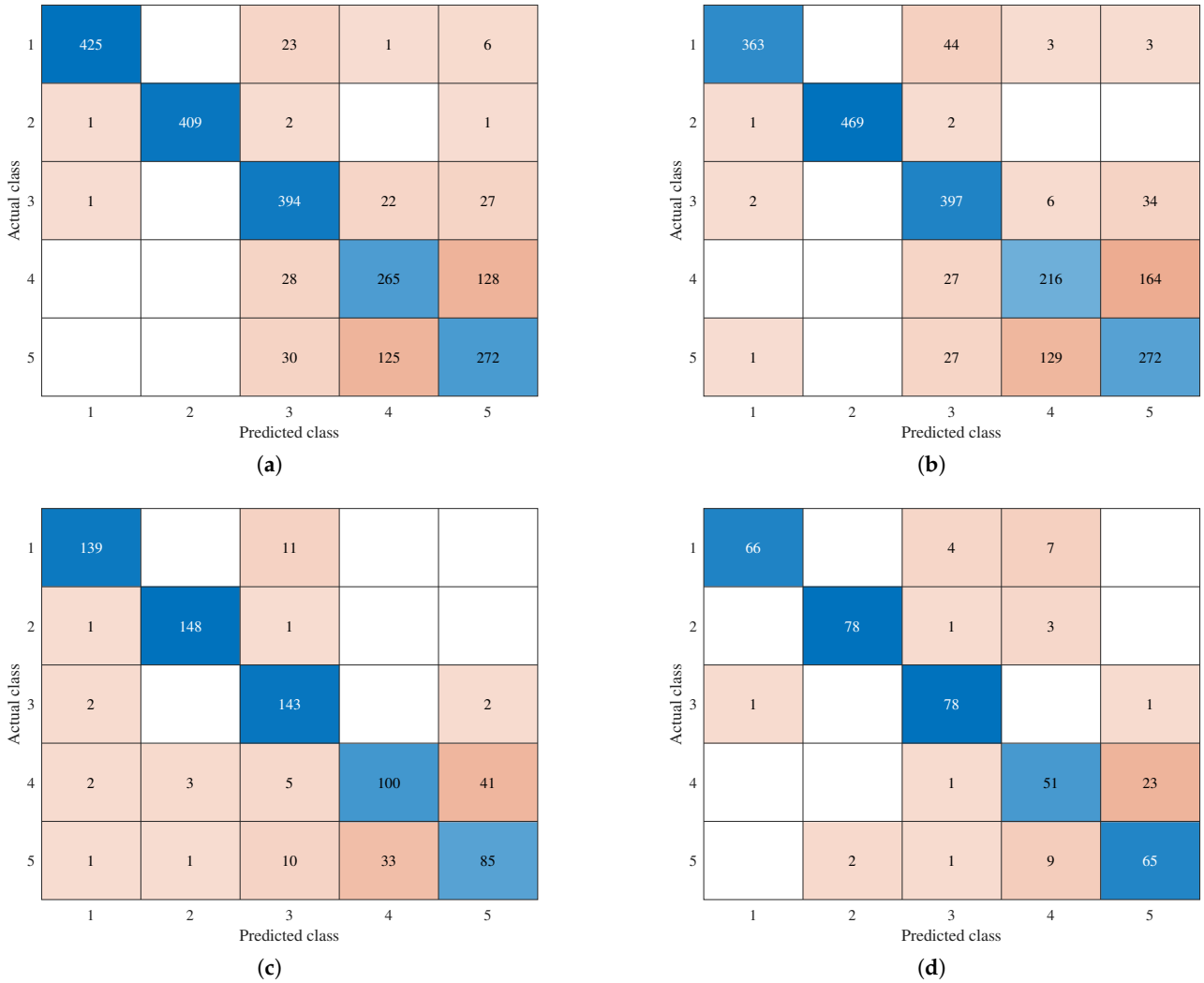
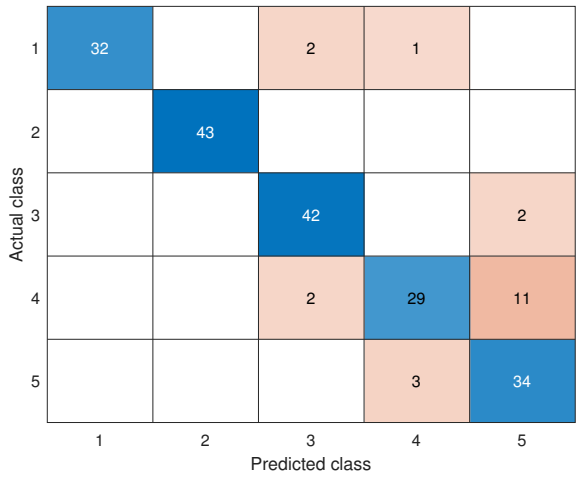


Figure 11. *Cont.*



(**e**)

Figure 11. Confusion matrices for the attack type classification results, with each subfigure representing experimental outcomes under different timeout conditions: (**a**) 15 s, (**b**) 20 s, (**c**) 60 s, (**d**) 120 s, (**e**) 240 s.

5. Conclusions

In this paper, we have focused on security issues in 5G core networks and proposed a DDoS attack detection model based on the Sin-Cos-bIAVOA algorithm, adapting Sin-Cos-bIAVOA from IoT DDoS detection to the 5G core network context. Through comparative experiments on a DDoS attack detection datasets for 5G core networks, the proposed detection model demonstrates superior performance across various attack scenarios, achieving higher detection accuracy than traditional DDoS detection algorithms. This provides a novel solution to the problem of DDoS attack detection in 5G core networks.

The Sin-Cos-bIAVOA algorithm demonstrates high accuracy for PFCP DDoS binary classification attack detection in the 5G core network, achieving an average accuracy of 97.948% in balanced traffic attack detection, outperforming other conventional algorithms. In multiclass experiments, the proposed algorithm is capable of accurately classifying both normal traffic and various types of attack traffic. Experimental tests show that the Sin-Cos-bIVOA algorithm can reach an accuracy of 89.552% and specificity of 97.4019% under a 240-s timeout.

This research indicates that a longer timeout allows the algorithm to more thoroughly process and analyze data, thereby unearthing more valuable feature information and enabling more precise classification and identification of attack types. However, in practical applications it is also necessary to consider the potential drawbacks of excessively long timeouts, such as increased resource consumption. Thus, selecting the most appropriate timeout setting based on specific scenario requirements is crucial in order to achieve an optimal balance between performance and resource utilization while effectively ensuring the security and stability of the network system. Further research will focus on performing more granular analyses of detection performance under various timeout conditions for different types of attacks as well as on exploring other factors that may influence algorithm performance, with the aim of continuously refining and improving the attack detection and classification algorithm to enhance its applicability and effectiveness in complex and dynamic cybersecurity environments.

Future efforts will focus on further exploring and optimizing this detection model, enhancing its adaptability and accuracy, and improving the concurrent execution efficiency of DDoS attack detection in 5G core networks. This effort is aimed at addressing the new challenges posed to 5G core network security by complex application scenarios such as large bandwidth, low latency, and terminal roaming.

Author Contributions: Conceptualization, Z.M.; methodology, Z.M.; software, Z.M.; validation, Z.M., R.Z. and L.G.; formal analysis, L.G.; investigation, L.G.; resources, L.G.; data curation, R.Z.; writing—original draft preparation, R.Z.; writing—review and editing, Z.M.; visualization, L.G.; supervision, L.G.; project administration, L.G.; funding acquisition, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the University–Industry Collaborative Education Program of the Ministry of Education of China grant number 231101020130957.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are openly available in [IEEE Dataport] at http://doi.org/10.21227/e0gj-ev03 (accessed on 11 February 2025), reference number [32].

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5GCN	5G Core Network
AMF	Access Management Function
AUSF	Authentication Server Function
CU	Centralized Unit
DL	Deep Learning
DU	Distributed Unit
gNB	gNodeB
IEs	Information Elements
ML	Machine Learning
MTD	Moving Target Defense
NEF	Network Exposure Function
NFV	Network Functions Virtualization
NRF	Network Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PFCP	Packet Forwarding Control Protocol
RAN	Radio Access Networks
SEID	Session Endpoint ID
SDN	Software-Defined Network
SMF	Session Management Function
UDM	User Data Management
UE	User Equipment
UPF	User-Plane Function

References

1. Pleshakova, E.; Osipov, A.; Gataullin, S.; Gataullin, T.; Vasilakos, A. Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. *J. Comput. Virol. Hacking Tech.* **2024**, *20*, 429–440. [CrossRef]
2. Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. *Sensors* **2021**, *21*, 16. [CrossRef] [PubMed]
3. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
4. Patil, R.; Tian, Z.X.; Gurusamy, M.; McCloud, J. 5G core network control plane: Network security challenges and solution requirements. *Comput. Commun.* **2025**, *229*, 107982. [CrossRef]

5. Choi, T.; Kim, T.; Tavernier, W.; Korvala, A.; Pajunpää, J. Agile Management and Interoperability Testing of SDN/NFV-Enriched 5G Core Networks. *ETRI J.* **2018**, *40*, 72–88. [CrossRef]
6. Kim, E.; Choi, Y.I. Traffic monitoring system for 5G core network. In Proceedings of the 11th International Conference on Ubiquitous and Future Networks (ICUFN), Zagreb, Croatia, 2–5 July 2019.
7. Lu, X.; Wang, X.; Pang, L.; Liu, J.; Yang, Q.; Song, X. Deployment and Reconfiguration for Balanced 5G Core Network Slices. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2021**, *104*, 1629–1643. [CrossRef]
8. Pell, R.; Shojafar, M.; Kosmanos, D.; Moschoyiannis, S. Service Classification of Network Traffic in 5G Core Networks using Machine Learning. In Proceedings of the 7th IEEE International Conference on Edge Computing and Communications (IEEE EDGE)/IEEE World Congress on Services (SERVICES), Chicago, IL, USA, 2–8 July 2023.
9. Oh, B.H.; Vural, S.; Rahulan, Y.; Wang, N.; Tafazolli, R. Performance Evaluation of a Virtualized 5G Core Network in Indoor Environments. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 19–21 June 2018.
10. Pinto, A.; Santaromita, G.; Fiandrino, C.; Giustiniano, D.; Esposito, F. Characterizing Location Management Function Performance in 5G Core Networks. In Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (IEEE NFV-SDN), Chandler, AZ, USA, 14–16 November 2022.
11. Zhu, X.T.; Qu, X.M. Research on 5G Lightweight Core Network Technology for Vertical Industries. In Proceedings of the 17th IEEE International Wireless Communications and Mobile Computing Conference (IEEE IWCMC), Harbin City, China, 28 June–2 July 2021.
12. Vanichchanunt, P.; Yamyuan, I.; Sasithong, P.; Wuttisittikulkij, L.; Paripurana, S. Implementation of Edge Servers on an Open 5G Core Network. In Proceedings of the 37th International Conference on Information Networking (ICOIN), Bangkok, Thailand, 11–14 January 2023.
13. Zieba, M.; Natkaniec, M.; Borylo, P. Cloud-Enabled Deployment of 5G Core Network with Analytics Features. *Appl. Sci.* **2024**, *14*, 25. [CrossRef]
14. Le, T.N.L.; Salem, B.A.; Ahad, E.A.; Aitsaadi, N.; Du, X. 5G-IoT-IDS: Intrusion Detection System for CIoT as Network Function in 5G Core Network. In Proceedings of the IEEE Conference on Global Communications (IEEE GLOBECOM)—Intelligent Communications for Shared Prosperity, Kuala Lumpur, Malaysia, 4–8 December 2023.
15. Huang, H.O.; Chu, J.F.; Cheng, X.C. Trend Analysis and Countermeasure Research of Ddos Attack under 5g Network. In Proceedings of the 5th IEEE International Conference on Cryptography, Beijing Normal University, Zhuhai, China, 8–10 January 2021.
16. Onoja, D.; Hitchens, M.; Shankaran, R. Security Policy to Manage Responses to Ddos Attacks on 5g Iot Enabled Devices. In Proceedings of the 13th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 21–23 June 2022.
17. Mamolar, A.S.; Pervez, Z.; Wang, Q.; Alcaraz-Calero, J.M. Towards the Detection of Mobile Ddos Attacks in 5g Multi-Tenant Networks. In Proceedings of the 28th European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019.
18. Mamolar, A.S.; Salvá-García, P.; Chirivella-Perez, E.; Pervez, Z.; Calero, J.M.A.; Wang, Q. Autonomic Protection of Multi-Tenant 5g Mobile Networks against Udp Flooding Ddos Attacks. *J. Netw. Comput. Appl.* **2019**, *145*, 102416. [CrossRef]
19. Ramezan, G.; Abdelnasser, A.; Liu, B.Y.; Jiang, W.Y.; Yang, F. Eap-Zkp: A Zero-Knowledge Proof Based Authentication Protocol to Prevent Ddos Attacks a the Edge in Beyond 5g. In Proceedings of the IEEE 4th 5G World Forum (5GWF), Montreal, QC, Canada, 13–15 October 2021.
20. Park, S.; Cho, B.; Kim, D.; You, I. Machine Learning Based Signaling Ddos Detection System for 5g Stand Alone Core Network. *Appl. Sci.* **2022**, *12*, 12456. [CrossRef]
21. Peng, C.; Fan, W.; Huang, W.Q.; Zhu, D.L. A Novel Approach Based on Improved Naive Bayes for 5g Air Interface Ddos Detection. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, UK, 26–29 March 2023.
22. Aljebreen, M.; Alrayes, F.S.; Maray, M.; Aljameel, S.S.; Salama, A.S.; Motwakel, A. Modified Equilibrium Optimization Algorithm with Deep Learning-Based Ddos Attack Classification in 5g Networks. *IEEE Access* **2023**, *11*, 108561–108570. [CrossRef]
23. Javadpour, A.; Ja'fari, F.; Taleb, T.; Benzaïd, C. Reinforcement Learning-Based Slice Isolation against Ddos Attacks in Beyond 5g Networks. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 3930–3946. [CrossRef]
24. Bousalem, B.; Silva, V.F.; Langar, R.; Cherrier, S. Ddos Attacks Detection and Mitigation in 5g and Beyond Networks: A Deep Learning-Based Approach. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Rio de Janeiro, Brazil, 4–8 December 2022.
25. Bousalem, B.; Silva, V.F.; Langar, R.; Cherrier, S. Deep Learning-Based Approach for Ddos Attacks Detection and Mitigation in 5g and Beyond Mobile Networks. In Proceedings of the 8th IEEE International Conference on Network Softwarization (NetSoft)—Network Softwarization Coming of Age—New Challenges and Opportunities, Politecnico Milano, Dipartimento Elettronica, Informazione & Bioingegneria, Milan, Italy, 27 June–1 July 2022.
26. Almiani, M.; AbuGhazleh, A.; Jararweh, Y.; Razaque, A. Ddos Detection in 5g-Enabled Iot Networks Using Deep Kalman Backpropagation Neural Network. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3337–3349. [CrossRef]

27. Sheikhi, S.; Kostakos, P. Ddos Attack Detection Using Unsupervised Federated Learning for 5g Networks and Beyond. In Proceedings of the Joint European Conference on Networks and Communications/6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 6–9 June 2023.
28. Fang, L.M.; Zhao, B.; Li, Y.; Liu, Z.; Ge, C.P.; Meng, W.Z. Countermeasure Based on Smart Contracts and Ai against Dos/Ddos Attack in 5g Circumstances. *IEEE Netw.* **2020**, *34*, 54–61. [CrossRef]
29. Kuang, X.; Hou, J.; Liu, X.; Lin, C.; Wang, Z.; Wang, T. Improved African Vulture Optimization Algorithm Based on Random Opposition-Based Learning Strategy. *Electronics* **2024**, *13*, 3329. [CrossRef]
30. Kaithal, P.K.; Sharma, V. African Vulture Optimization-Based Decision Tree (AVO-DT): An Innovative Method for Malware Identification and Evaluation through the Application of Meta-Heuristic Optimization Algorithm. *Cybern. Inf. Technol.* **2024**, *24*, 142–155. [CrossRef]
31. Kholidy, H.A.; Karam, A.; Sidoran, J.L.; Rahman, M.A. 5G Core Security in Edge Networks: A Vulnerability Assessment Approach. In Proceedings of the 26th IEEE Symposium on Computers and Communications (IEEE ISCC), Athens, Greece, 5–8 September 2021.
32. Amponis, G.; Radoglou-Grammatikis, P.; Nakas, G.; Goudos, S.; Argyriou, V.; Lagkas, T.; Sarigiannidis, P. 5G Core PFCP Intrusion Detection Dataset. In Proceedings of the 2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST), Athens, Greece, 28–30 June 2023; pp. 1–4.
33. Amponis, G.; Radoglou-Grammatikis, P.; Lagkas, T.; Ouzounidis, S.; Zevgara, M.; Moscholios, I.; Goudos, S.; Sarigiannidis, P. Generating full-stack 5G security datasets: IP-layer and core network persistent PDU session attacks. *AEU Int. J. Electron. Commun.* **2023**, *171*, 154913. [CrossRef]
34. Ock, J.; No, H.; Kim, S. Poster: Exploring Synthetic Data Generation for Anomaly Detection in the 5G NWDAF Architecture. In Proceedings of the 43rd IEEE International Conference on Distributed Computing Systems, ICDCS 2023, Hong Kong, China, 18–21 July 2023.
35. Sarhan, M.; Layeghy, S.; Moustafa, N.; Portmann, M. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*; Springer: Berlin/Heidelberg, Germany, 2024; Volume 371, pp. 117–135.
36. Samarakoon, S.; Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Chang, S.-Y.; Kim, J.; Kim, J.; Ylianttila, M. 5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network. *arXiv* **2022**, arXiv:2212.01298. [CrossRef]
37. Sharma, N.; Shambharkar, P.G. Transforming security in internet of medical things with advanced deep learning-based intrusion detection frameworks. *Appl. Soft Comput.* **2025**, *180*, 113420. [CrossRef]
38. Moubayed, A. A Complete EDA and DL Pipeline for Softwarized 5G Net Moubayed, A.work Intrusion Detection. *Future Internet* **2024**, *16*, 331. [CrossRef]
39. Yuan, L.; Sun, J.; Zhuang, S.; Liu, Y.; Geng, L.; Ma, W. CoSen-IDS: A Novel Cost-Sensitive Intrusion Detection System on Imbalanced Data in 5G Networks. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2024; Volume 14869, pp. 470–481.
40. Civciss, A.; Ravihansa, V.; Sandeepa, C.; Liyanage, M. Netslab-5G-ORAN-IDD [Data Set]. Kaggle. 2025. Available online: https://www.kaggle.com/datasets/netslabdemo/netslab-5g-oran-idd (accessed on 11 June 2025).
41. Abdollahzadeh, B.; Gharehchopogh, F.S.; Mirjalili, S. African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems. *Comput. Ind. Eng.* **2021**, *158*, 107408. [CrossRef]
42. Gharehchopogh, F.S.; Ibrikci, T. An improved African vultures optimization algorithm using different fitness functions for multi-level thresholding image segmentation. *Multimed. Tools Appl.* **2024**, *83*, 16929–16975. [CrossRef]
43. Xiao, Y.; Guo, Y.; Cui, H.; Wang, Y.; Li, J.; Zhang, Y. IHAOAVOA: An improved hybrid aquila optimizer and African vultures optimization algorithm for global optimization problems. *Math. Biosci. Eng.* **2022**, *19*, 10963–11017. [CrossRef] [PubMed]
44. Zheng, R.; Hussien, A.G.; Qaddoura, R.; Jia, H.; Abualigah, L.; Wang, S.; Saber, A. A multi-strategy enhanced African vultures optimization algorithm for global optimization problems. *J. Comput. Des. Eng.* **2023**, *10*, 329–356. [CrossRef]
45. Sharifian, Z.; Barekatain, B.; Quintana, A.A.; Beheshti, Z.; Safi-Esfahani, F. Sin-Cos-bIAVOA A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection. *Expert Syst. Appl.* **2023**, *228*, 120404. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.