Influence of DDoS Attacks on Resource Allocation in Three-Dimensional 6G Networks

Maria G. Lima Damasceno*†, Renata K. Gomes dos Reis*†, Caio B. Bezerra De Souza*†, Jussif J. Abularach Arnez†, Andson Balieiro*, Kelvin Lopes Dias*

*Centro de Informática (CIn), Universidade Federal de Pernambuco (UFPE), Recife, Brazil

†Sidia Institute of Science and Technology, Manaus, Brazil.

Email: {*†maria.lima, *†renata.gomes, *†caio.souza,† jussif.arnez}@sidia.com, {*amb4, *kld}@cin.ufpe.br

***Abstract*—Three-dimensional (3D) Sixth Generation (6G) networks are expected to comprise a multitude of resources for allocation (e.g., power, computing, and radio resources) in devices heterogeneous (e.g., height, capacity, and connectivity) at different layers (e.g., terrestrial and aerial). This complexity increases the possibilities for Distributed Denial of Service (DDoS) attacks, boosting their effects. This paper presents a review on the effects of DDoS attacks on resource allocation (RA) in 3D 6G networks. It analyzes the related studies regarding the problems and resoures they deal with, their features, author's assumptions, and metrics adopted in their evaluation. In addition, this paper points out challenges and opportunities that may be addressed in resource allocation in 3D 6G networks when facing DDoS attacks.**

***Index Terms*—3D 6G Networks, DDoS attacks, Non-Terrestrial Networks**

I. Introduction

While the Fifth Generation of Mobile Networks (5G) has been implemented around the world, the industry and academia are already conducting studies regarding the Sixth Generation (6G) [1]. 6G networks are expected to provide ultra-high data rate of 1 Tbps, ultra-low latency of 0.1 ms, low energy consumption, mobility support of up to 1000km/hr, zero-touch network automation, and improve coverage area percentage to 99%, enabling applications not yet supported by the 5G networks and new ones such as digital twins, metaverse, and holographic communications [2], [3].

To enable the 6G networks, a multitude of technologies are envisioned such as THz communication, Federated Learning (FL), edge AI, Compressive Sensing (CS), Blockchain/Distributed Ledger Technologies (DLT), Non-Terrestrial Networks (NTN) for 3D networking, carrier aggregation, network slicing, network function virtualization (NFV), and multiple levels of cloud computing [4]. Given the challenges faced by 5G Terrestrial Networks (TN) in providing global connectivity and meeting performance requirements [5], the next generation is a genuine candidate to efficiently support NTN and 3D networking [6]. NTN expands the TN connectivity by adding a third dimension and providing higher coverage, trunking, backhauling and supporting high-speed mobility in unserved or underserved areas through the integration of aerial components such as Unmanned Aerial Vehicles (UAVs) and satellites with ground platforms. Embedding computing resources into aerial devices expands the network capacity to handle heavy computational tasks, decreasing user energy consumption and bandwidth features, and providing line-of-sight transmissions [7] [8]. Additionally, this approach makes the system less susceptible to serious damage and service capacity losses caused by natural such as landslides and earthquakes [9].

The diversity of end devices, network elements, protocols, services, and technologies will make the 3D 6G Networks more complex and sophisticated, and will expand vulnerability points and threats for cybernetic attacks. Consequently, dimensioning, managing, and operating these networks safely will be a challenge [10]. In this respect, the 6G ecosystem has advocated the use of Artificial Intelligence (AI) and Machine Learning (ML) techniques for Resource Allocation (RA) and other activities in 6G networks. However, these techniques could also lead to security breaches, where trained AI models can be attacked by malicious users to degrade their accuracy, thus affecting the System Quality of Service (QoS), or infect devices to launch Distributed Denial of Service (DDoS) attacks [11]. Additionally, for 3D scenarios, where there is a multitude of resources for allocation (e.g., power, computing, and radio resources) in devices heterogeneous (height, capacity, connectivity) at different layers (e.g., terrestrial and aerial), the possibilities for DDoS attacks raise and their effects may be boosted [12]. Recent studies have analyzed AI-based approaches for 5G/6G networks, NTN, and security, such as [13], [5], [2], and [11]. For instance, [13] reviews the state-of-art of AI-based resource management solutions and highlights challenges for deploying AI techniques in 5G/6G networks. The authors evaluate radio and computing resource management solutions from three perspectives: Mobile Network Operators (MNO) and micro-operators, network slicing, and cognitive radio. Regarding radio resources, they deal with spectrum, power, and channel assignments, but overlook NTN scenarios or security issues, and neglect solutions for computing resources management.

The authors in [5] provide a comprehensive review of the control objectives required by NTN elements exploring Reinforcement Learning (RL) techniques. They analyze the level of realism of studies based on simulation, station deployment setting, wireless channel and energy assumptions. [2] introduces new paradigms for the next generations of

mobile networks related to air computing, and presents a dynamic and high-resolution computing and communication environment for 6G networks. On the other hand, [11] provides a comprehensive overview of security and privacy threats in the 6G network edge. The paper highlights the vulnerability of 5G applications against DDoS attacks due to the limited communication and computation resources, but fails to provide countermeasures to address them in 6G networks.

In this respect, this paper presents a review on NTN and security studies in 6G networks, seeking to answer how DDoS attacks could affect the resource allocation in 3D 6G networks. Additionally, we analyze the works regarding the problems and resoures they deal with, their features, author's assumptions, and metrics adopted in their evaluation. This paper also exposes challenges and opportunities that may be addressed in resource allocation in 3D 6G networks when facing DDoS attacks. This paper is organized as follows. Section II presents key concepts related to NTN and DDoS attacks. The analysis of the studies is carried out in Section III, where aspects such as addressed problem, solution assumptions, and evaluation metrics are highlighted. Challenges and Opportunities are pointed out in Section IV. Section V concludes this paper.

II. Key Concepts

This section discusses key concepts in 3D 6G networks and security, highlighting their main points and connections.

A. NTN and 3D Networks

Three-dimensional networks integrate the existing TN to aerial platforms and satellite networks to provide wider coverage, longer endurance, and high payload capabilities. In particular, satellite networks consist of different types of orbit, such as Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO). On the other hand, aerial networks are divided into several layers, for instance, High Altitude Platform (HAP) and Low Altitude Platform (LAP). The former comprises airplanes or high-altitude UAVs, ranging from 20 Km to 50 Km of altitude, while the latter typically refers to small unmanned airplanes, having short mission durations and operating at low altitudes [14] [4] [15]. Due to its highly dynamic components, this structure provisioned by Three-dimensional 6G networks brings several challenges for resource allocation, such as severe bandwidth shortage and high transmission power battery consumption.

B. Resources in 3D 6G Networks

Due to the high heterogeneity of 3D 6G networks, a large amount of radio and computational resources will be available to support the massive volume of devices and applications in addition to the integration of different technologies, including Cloud Computing, Multi-access edge computing (MEC), and NTN. Thus, dealing with different services may require the allocation of computing resources such as virtual machines, containers, CPU (core, cycle, quantum, or fraction), physical memory and storage, besides communication ones, where bandwidth (spectrum frequency, channel, and time slot), transmission power, and radio interfaces are examples of resources that may be managed to provide wireless connectivity to mobile users [1]. The network core is mainly responsible for managing network resources and user connections, such as authentication, security and others. Resource allocation can be viewed as a two-stage process: dimensioning and operation. In the dimensioning stage, a certain amount of resources is assigned to a group of users, classes, or the network before network operation, i.e., statically. In contrast, the operation stage involves allocating resources to individual users or traffic flows while the network is operational, i.e., dynamically. This dynamic allocation may be performed based on user priority and system availability, among other factors.

C. DDoS Attacks

Denial of Service (DoS) and, more specifically, DDoS attacks have increased in recent years in both frequency and traffic volume, with outbreaks reaching rates on the order of terabits per second and compromising the availability of various infrastructures [16]. When it comes to 3D networks that comprise multiple interconnected aerial and terrestrial devices [5], these attacks can amplify their effects. For instance, in a DDoS attack against a 3D network, a malicious machine can control a set of other ones to overload target devices such as airplanes, satellites, UAVs or base stations, as seen in Fig. 1.

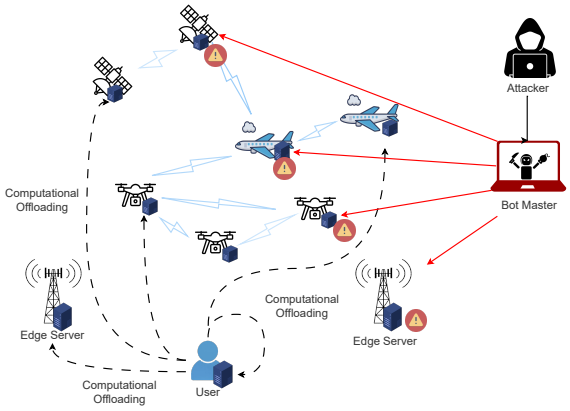

Fig. 1. DDoS attack during computational offloading.

Moreover, the use of Software Defined Networking (SDN) in 3D networks may simplify their management but also increases security problems due to the lack of flexibility and programmability of the data plan, which is usually the first to suffer DDoS [17]. Thus, studying the effects of these attacks on SDN-based 3D 6G networks is necessary, particularly concerning resource allocation.

III. Current Research

This section addresses solutions for 6G Resource Allocation (RA) and DDoS/DoS attacks in NTN and 3D networks, considering the Included Studies (IS) exhibited in Table I. They are analyzed regarding their addressed problems (Section III-A), assumptions (Section III-B), features (Section III-C), and metrics (Section III-D).

A. Addressed Problems

Existing literature discusses several issues associated with the allocation of radio and computational resources, and security in 3D 6G networks, comprising Distributed Resource Allocation (DRA), computational offloading, energy consumption and vehicle trajectory optimization, scheduling and DoS/DDoS attacks, as shown in Table I. For instance, IS3, IS5, IS16, IS17, and IS18 propose different strategies for computing offloading in which IS3 considers partial offloading and total local computing, evaluating task energy consumption and delay based on user available computing resources and CPU cycles. In contrast, IS5 proposes a total offloading solution, disregarding the availability of the MEC-UAV connection while it is moving. Moreover, this study defines its offloading strategy to remote and local execution scenarios based on the task completion time. On the other hand, IS16 deals with the computing offloading problem from the routing perspective, proposing a cloud selection and routing optimization as a DRA in which both wired and wireless MEC links are considered.

The successive studies IS2, IS4, IS6, IS17 and IS8 focus on radio resource allocation in 6G heterogeneous networks (HetNets), NTN, and 3D networks. IS2 optimizes uplink transmit power and provides a traffic scheduling technique that aims to allocate power and spectrum resources in an optimal way. IS4 proposes non-orthogonally resource sharing of Access Link (AL) and Backhaul Link (BL) bandwidth in a 3D aerial network, considering that UAVs may assume two roles, an aerial BS or an aerial UE. Different from IS2 and IS4, IS6 applies Deep Reinforcement Learning (DRL) for radio resource allocation in 6G HetNets with semi-centralized cloud topology, taking into consideration a variety of input parameters, including available power, bandwidth, Signal-to-Noise Ratio (SNR), QoS demands, and Channel State Information (CSI). Studies IS17 and 18 embedd MEC technology into LEO satellites to handle heavy computational tasks, saving energy consumption and bandwidth resources, without transmission delay that may be caused by natural disasters.

Efforts have been done by IS3, IS5, IS12, IS2, and IS16 to jointly allocate resources and optimize energy consumption and UAV trajectory. The first three studies address the vehicle trajectory to assist terrestrial devices during resource allocation procedures. Particularly, IS12 determines the UAV position distribution aiming to improve coverage while computational resources are assigned. IS2 and IS16 explore energy consumption optimization methods, but IS16 ovlerlooks the energy consumed by routers in its solution. Works such as IS1 and IS17 propose new 3D 6G network architectures and highligth their impacts on QoS metrics. The former suggests a decentralized and a ground-centralized core network to support broadband communication and Large-Scale IoT services. The latter propose a direct connectivity and local offloading scenarios with LEO satellite backhaul.

As observed, these previous solutions address resource allocation, trajectory optimization, or routing selection problems while considering secure network environments, i.e., without taking into account the possibility of attack occurrences and their impact on the solution performance. However, when the network elements are facing cyber attacks, such as DDoS one, the solutions may make errouneous decisions and have their performance degraded. For instance, since a UAV-based MEC node is an energy and computing-constrained device, it requires a careful definition on its trajectory and use of resources. So, when malicious users request resources from a UAV-based MEC node in a 3D network managed by solutions without safety awareness, they could receive resources, causing starvation for legitimate ones and service unavailability. Additionally, they may lead to wasting UAV energy as the aerial device may take a route to cover the malicious users. This can result in frequent UAV recharges or damage to the device when its energy is depleted during flight. In terms of security, IS8 and IS10 describe problems related to the lack of flexibility of SDN networks, highlighting that these networks can be susceptible to DDoS attacks. In IS11, the authors argue that adversarial attacks may cause significant damage to cyber-physical systems (CPSs), as these systems are often applicable to healthcare equipment and energy systems. IS13 raises the issue that IoT devices are resource-constrained, so protecting them when security mechanisms at the gateway fail is challenging and it has implications for 3D networks under DDoS attacks.

B. Assumptions

The previous section discussed solutions for different problems in 3D 6G Networks. These solutions are designed based on some assumptions, which are important to be analyzed from the security perspective, particularly, when the networks face DDoS attacks. For instance, IS1 assumes a ground-centralized core network scenario where network functions such as Access Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) may all be placed on the air platform along with the Radio Resource and Bearer Management Control Function (RRBMCF), and Packet Data Unit and Sessions Function (PDUSF). This configuration may provide a full network embedded into a UAV platform, for example, but in case of DDoS atrack, all network segments (core and radio access) might be unavailable or there might not be enough resources to replicate the network functions under attack, given that UVAs are resource-limited devices.

Studies IS3, IS5, IS16, IS17, and IS18 deal with task offloading, where some consider that a task may be only processed remotely (total offloading), while others assume they are divided into subtasks to be served by different computing nodes, including the user device (partial offloading), which eventually may process the whole (total local offloading). From the perspective of a system that adopts a total offloading strategy under DDoS attacks, the computing node tends to receive larger tasks, which may consume its resources faster. However, at the same time, the number of users being attended is fewer, which may ease the detection and mitigation of the attack. On the other hand, by adopting partial offloading, the computing node tends to deal with a larger amount of

smaller requests from diverse nodes, which may make the attack detection more challeging and affect more legitime users that share the computing node under attack. Additionally, the attacker may require more malicious node to employ the attack.

Among the analyzed studies on task offloading, only IS5 presumes a system with task failures, as shown Table I, but it does not employ any mechanism to mitigate their effects on the service performance or resource allocation. Adopting task replication during resource allocation is an alternative to mitigate the DDoS effects on the service perfomance. It allows copies of an subtask to be processed in differente nodes, improving the service realibilty besides lowering the response time, but at the cost of using more resources to attend the users, which may reduce the system capacity. Besides the computing resources, the transmission ones may be attacked via DDoS offensives, which must be considerd in the designing of solutions and depends on the assumed transmission directions. Studies such as IS2, IS3, IS4, IS7, IS16, and IS18, propose solutions that work in only one direction (uplink or downlink), while others deal with both ones (e.g.,IS1 and IS17). Restricting the direction of communication may reduce the concern of attack but limits the applicability of the solution. For instance, computational offloading solutions that just address uplink communication (e.g., IS3) are not recommended for applications that send a significant amount of data back to the user, such as video editing. In such cases, resources need to be allocated and the cost of downlink considered. This limitation may lead to a performance gap and potential downlink channel overload.

C. Features and Characteristics

Table I shows that the majority solutions for adversarial attacks found in studies related to DoS or DDoS attacks use AI/ML, as seen in IS10 and IS13. Phyton and MATLAB are the preferred simulation tools for different designig solutions for different problems while emulation is adopted in IS8, IS9, IS10, and IS17 to analyze their proposals. In terms of mathematical tools and heuristics, game theory is adopted for resource scheduling in IS14, IS15, and IS16 while Markov Decision Process (MDP) is employed in IS11 and IS18 for DDoS attacks and offloading decision, respectively. In addition, a binary particle swarm optimization (PDPSO) and a two-stage heuristic (SUM) with an clustering algorithm (TSS-DBSCAN) are proposed to optimize the UAV trajectory in IS3, and also allocate the computacional resources in IS5, respectively. IS10, in turn, adopts mathematical (KL) and AI/ML (RBM) tools to address both DoS and DDoS attacks in an emulated environment, in which the SDN controller is responsible to block domains IP on which the DDoS attacks are originated. Among the solutions analyzed, it is worth noting that in the studies on adversarial attacks, there is limited explanation regarding the network segment that is being targeted or affected. In terms of network segment, the studies IS1, IS2, IS4, IS6, IS7, IS8 and IS15 address the Radio Access Networks (RAN), which provides connection between the mobile network core and end users, mainly describing 6G and NTN networks. IS14 and IS16 propose Game Theory-based solutions for resource allocation in MEC architecture, while IS3 and IS5 deal with UAV-based MEC system. Finally, studies IS17 and IS18 describe the MEC-LEO network segment from the perspective of resource allocation and task offloading.

D. Evaluation Metrics

Positioning the core network on the TN and supplying the access network using over-air-platforms have shown that data forwarding delay and control message transmission delay are both quite significant since all user traffic data and control messages must be routed back to the ground for processing. When the network functions are embedded into air nodes, the service transmission delay and the system robustness may be improved. Table II summarizes the metrics used in the analyzed studies. We may note that IS3 and IS5 adopt the majority of metrics for task offloading and UAV trajectory. Few studies consider quality of service metrics such as Delay and Throughput. These metric are analyzed in IS2 and IS3 along with energy consumption.

IV. Challenges and Opportunities

The resource allocation in 3D 6G networks presents challenges that must be addresses in order to provide efficient and safety networks. One notable issue observed in our review is the absence of comprehensive studies that analyze the effects of DDoS attacks on resource allocation in the next generation of mobile communications. This issue may be tackled from different perspectives, such as per network segment, operator view, service performance, and network layer (terrestrial or aerial). This lack of analysis may stem from another issue, namely, the few solutions for resource allocation take into account the occurrence of DDoS attacks in their scope. Many of the analyzed studies focus on efficient resource allocation and trajectory optimization, for example, but overlook security aspects, especially DDoS events. On the other hand, there are studies that aim to detect and mitigate DDoS attacks but do not consider the resource allocation process in their approaches. Thus, designing security-aware AI/ML-based solutions for resource allocation is of paramount importance in 3D 6G networks. These solutions must not only provide efficient resource allocation and be robust against cybernetic attacks (e.g., DDoS) on network resources/nodes but also protect their own structure from adversarial offensives [10].

V. Conclusion

This paper offered a qualitative analysis on the influence of DDoS attacks on resource allocation in 3D 6G networks. We discussed the studies regarding the problems and assumptions that they deal with besides their main features and evaluation metrics. It was noted the use of game theory and AI/ML solutions for resource optimization problems, where in scenarios involving UAVs, the energy consumption is an important analyzed metric analized, although the authors in task offloading problems just consider the uplink communication and overlook

TABLE I
FEATURES AND CHARACTERISTICS OF THE ANALYZED STUDIES

ID	Work	Problem Adress	Network Segment	Mathematical Tool	AI/ML	Simulation	Emulation
IS1	[18]	3D Network Orchestration	RAN, CORE	N/A	N/A	N/A	N/A
IS2	[19]	Energy Optimization, Resource Scheduling	RAN	Segmentation algorithm, Heuristic Scheduler	N/A	MATLAB	N/A
IS3	[20]	Trajectory Optimization, Offloading	MEC-UAV	PDPSO	DDPG	Python	N/A
IS4	[12]	Resource Scheduling	RAN	NSRA	N/A	N/A	N/A
IS5	[21]	Trajectory Optimization, Offloading	MEC-UAV	SUM, TSS-DBSCAN	N/A	N/A	N/A
IS6	[1]	Radio Resource Optimization	RAN	N/A	DRL	N/A	N/A
IS7	[22]	Radio Resource Allocation	RAN	N/A	QML	N/A	N/A
IS8	[23]	DoS Attack Detection and Mitigation	RAN	N/A	N/A	N/A	DPPSN
IS9	[16]	DDoS Attack Detection and Mitigation	N/A	Shannon Entropy	N/A	N/A	CAIDA Dataset, P4
IS10	[17]	DoS and DDoS Attack Detection	N/A	KL	RBM	N/A	OpenFlow
IS11	[24]	DoS Attacks Optimization	N/A	SINR Model, MDP	N/A	N/A	N/A
IS12	[25]	Trajectory Optimization	N/A	EO, SMA	K-Means	hping3	N/A
IS13	[26]	DoS Attack Detection and Mitigation	N/A	N/A	K-Means	Pyhton, SUMO	N/A
IS14	[7]	Resource Scheduling	MEC	Game Theory, DBSCAN	N/A	MATLAB	N/A
IS15	[8]	Resource Allocation	RAN	Game Theory	N/A	N/A	N/A
IS16	[27]	Energy Optimization, Resource Scheduling, Routing, Offloading	MEC	Game Theory, Optimization Algoritm	N/A	N/A	N/A
IS17	[28]	3D Network Orchestration, Offloading	MEC-LEO (RAN, CORE)	N/A	N/A	N/A	OpenSand, Amarisoft, Open5gs
IS18	[9]	Resource Allocation, Offloading	MEC-LEO	MDP	DDPG-LSTM	Python	N/A

task failure occurrences, and the UAV mobility cost. The study also highlighted challenges that may be addressed in this topic, such as the scarcity of security-aware solutions for resource allocation in the next generation of mobile communications.

ACKNOWLEDGMENT

This study was funded by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Code 001. This work was presented as part of the results of the Project: AMAN, executed by the Sidia Institute of Science and Technology, in partnership with Samsung Eletrônica da Amazônia LTDA, according to Informatics Law n.8387/91 and Art.39 of Decree 10.521/2020.

REFERENCES

[1] A. Alwarafy, A. Albaseer, B. S. Ciftler, M. Abdallah, and A. Al-Fuqaha, "AI-based radio resource allocation in support of the massive heterogeneity of 6G networks," in *2021 IEEE 4th 5G World Forum (5GWF)*. IEEE, 2021, pp. 464–469.

[2] B. Yamansavascilar, A. Ozgovde, and C. Ersoy, "Air computing: A survey on a new generation computation paradigm in 6G wireless networks," *arXiv preprint arXiv:2209.04640*, 2022.

TABLE II
STUDY ASSUMPTIONS AND EVALUATION METRICS

Model Assumptions and Metrics	IS1	IS2	IS3	IS4	IS5	IS6	IS7	IS8	IS9	IS10	IS11	IS12	IS13	IS14	IS15	IS16	IS17	IS18
UAV Always Available	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Partial Offloading	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Full Task Offloading	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Total Local Computing	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Task Failure	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Uplink Transmission	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
Downlink Transmission	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Throughput	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Delay	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
Re-routing time	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Energy/Power Consumption	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓
Model Accuracy	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓

[3] M. Banafaa, I. Shayea, J. Din, M. Hadri Azmi, A. Alashbi, Y. Ibrahim Daradkeh, and A. Alhammadi, "6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities," *Alexandria Engineering Journal*, vol. 64, pp. 245–274, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S111001682200549X

[4] C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 836–886, 2021.

[5] T. Naous, M. Itani, M. Awad, and S. Sharafeddine, "Reinforcement learning in the SKY: A survey on enabling intelligence in NTN -based communications," *IEEE Access*, vol. 11, pp. 19 941–19 968, 2023.

[6] M. Chen, J. Shao, X. Huang, L. Su, S. He, and H. Du, "Security analysis and improvement for satellite and mobile network integration," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*. IEEE, 2022, pp. 469–474.

[7] R. I. Meneguette and H. A. Prado Marques, "A game theory-based vehicle cloud resource allocation mechanism," *Revista Eletrônica de Iniciação Científica em Computação*, vol. 20, no. 2, jun. 2022. [Online]. Available: https://sol.sbc.org.br/journals/index.php/reic/article/view/2281

[8] S. Yan, M. Peng, and X. Cao, "A game theory approach for joint access selection and resource allocation in UAV assisted IoT communication networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1663–1674, 2019.

[9] H. Zhang, S. Xi, H. Jiang, Q. Shen, B. Shang, and J. Wang, "Resource allocation and offloading strategy for UAV-assisted LEO satellite edge computing," *Drones*, vol. 7, no. 6, 2023.

[10] C. Benzaïd and T. Taleb, "AIfor beyond 5G networks: A cyber-security defense or offense enabler?" *IEEE Network*, vol. 34, no. 6, pp. 140–147, 2020.

[11] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Communications Surveys Tutorials*, vol. 25, no. 2, pp. 1095–1127, 2023.

[12] J. Kim, H. Lee, and D. Hong, "A new resource management technique in 3D wireless networks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, 2023, pp. 1–5.

[13] M. Lin and Y. Zhao, "Artificial intelligence-empowered resource management for future wireless communications: A survey," *China Communications*, vol. 17, no. 3, pp. 58–77, 2020.

[14] A. Iqbal, M.-L. Tham, Y. J. Wong, A. Al-Habashna, G. Wainer, Y. Zhu, and T. Dagiuklas, "Empowering non-terrestrial networks with artificial intelligence: A survey," 06 2023.

[15] J. Qiu, D. Grace, G. Ding, M. D. Zakaria, and Q. Wu, "Air-ground heterogeneous networks for 5G and beyond via integrating high and low altitude platforms," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 140–148, 2019.

[16] C. Lapolli, J. Adilson Marques, and L. P. Gaspary, "Offloading real-time DDoS attack detection to programmable data planes," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 19–27.

[17] M. Klymash, O. Shpur, N. Peleh, and O. Maksysko, "Concept of intelligent detection of DDoS attacks in sdn networks using machine learning," in *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC ST)*, 2020, pp. 609–612.

[18] J. Wang, Y. Zhou, and B. Wang, "Design of 6G space-ground integrated network architecture based on ground core network," in *2023 International Wireless Communications and Mobile Computing (IWCMC)*, 2023, pp. 1250–1255.

[19] M. N. Dazhi, H. Al-Hraishawi, M. R. B. Shankar, S. Chatzinotas, and B. Ottersten, "Energy-efficient service-aware multi-connectivity scheduler for uplink multi-layer non-terrestrial networks," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 3, pp. 1326–1341, 2023.

[20] Y. Gan and Y. He, "Trajectory optimization and computing offloading strategy in UAV-assisted MEC system," in *2021 Computing, Communications and IoT Applications (ComComAp)*, 2021, pp. 132–137.

[21] Y.-H. Chao, C.-H. Chung, C.-H. Hsu, Y. Chiang, H.-Y. Wei, and C.-T. Chou, "Satellite-UAV-MEC collaborative architecture for task offloading in vehicular networks," in *2020 IEEE Globecom Workshops (GC Wkshps*, 2020, pp. 1–6.

[22] M. Shahjalal, W. Kim, W. Khalid, S. Moon, M. Khan, S. Liu, S. Lim, E. Kim, D.-W. Yun, J. Lee, W. Lee, S.-H. Hwang, D. Kim, J.-W. Lee, H. Yu, Y. Sung, and Y. M. Jang, "Enabling technologies for AIempowered 6G massive radio access networks," *ICT Express*, vol. 9, 07 2022.

[23] E. Kaljic, A. Maric, and P. Njemcevic, "DoS attack mitigation in sdn networks using a deeply programmable packet-switching node based on a hybrid FPGA/CPU data plane architecture," in *2019 XXVII International Conference on Information, Communication and Automation Technologies (ICAT)*, 2019, pp. 1–6.

[24] S. Zhang, L. Peng, and X. Chang, "Optimal energy allocation based on sinr under DoS attack," *Neurocomputing*, p. 127116, 2023.

[25] S. Barshandeh, S. Koulaeizadeh, M. Masdari, B. AbdollahZadeh, and M. Ghasembaglou, "A learning-based metaheuristic administered positioning model for 3D IoT networks," *Applied Soft Computing*, vol. 136, p. 110113, 2023.

[26] J. J. Kponyo, J. O. Agyemang, G. S. Klogo, and J. O. Boateng, "Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices," *Internet of Things*, vol. 12, p. 100319, 2020.

[27] B. Wu, J. Zeng, L. Ge, Y. Tang, and X. Su, "A game-theoretical approach for energy-efficient resource allocation in MEC network," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[28] P. Agbo-Adelowo and P. Weitkemper, "Analysis of different MEC offloading scenarios with LEO satellite in 5G networks," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, 2023, pp. 1–6.