Brief Report

Simulation of Attacks on UAV Swarm with Repeater

Volodymyr Kharchenko , Andrii Grekhov * , Vasyl Kondratiuk

Posted Date: 19 September 2025

doi: 10.20944/preprints202509.1726.v1

Keywords: UAV Swarm; DoS attacks; repeater; interference protection

 doi:10.20944/preprints202509.1726.v1

Brief Report

Simulation of Attacks on UAV Swarm with Repeater

Volodymyr Kharchenko [1], Andrii Grekhov [2,*] and Vasyl Kondratiuk [3]

[1] Research Training Center "Aerospace Center",State University "Kyiv Aviation Institute", Kyiv, Ukraine, Senior Member IEEE

[2] Research Training Center "Aerospace Center", State University "Kyiv Aviation Institute", Kyiv Kyiv, Ukraine

[3] Research Training Center "Aerospace Center", State University "Kyiv Aviation Institute", Kyiv, Ukraine

* Correspondence: grekhovam@gmail.com

Abstract

Study is devoted to the problem of interference protection for communication channels of Unmanned Aerial Vehicle (UAV) swarm during attacks, which is relevant due to the growth of threats in military and civilian applications (intelligence, monitoring, and logistics). The use of a repeater expands the range and coordination of the swarm, but increases vulnerability to attacks such as directional interference. A model was developed using NetCracker and includes Base Station, Repeater, Aerial Base Station, UAV swarm, and Attacker that simulates Denial-of-Service (DoS) attacks. The model allows analyzing the impact of interference on communication, taking into account Bit Error Rate (BER), delay, and throughput. The simulation results showed that at Time-Between-Transaction (TBT) of 0.01 s and Transaction Size (TS) of 100,000 bits, packet losses reach 30%. The novelty lies in the integration of networks with a repeater and real-time attack simulation, which fills the gaps in existing research.

Keywords: UAV Swarm; DoS attacks; repeater; interference protection

I. Problem Statement

The development and application of UAV swarms are actively developing in military and civilian areas, including reconnaissance, monitoring, agriculture and logistics. Using a repeater extends the communication range and improves swarm coordination, but at the same time increases the system's vulnerability to attacks. The relevance of this study is due to the growth of threats, an increase in the number of attacks on UAVs in military conflicts, the emergence of new methods of suppressing communications, such as directional interference.

UAV swarms require stable communication channels for self-organization and adaptation to losses. The loss of a repeater can lead to complete disorganization of the swarm. Modern communication systems are vulnerable to interference, which reduces the effectiveness of the swarm. Modeling attacks allows to predict the behavior of the swarm in counteraction, optimize control algorithms and increase interference immunity, which is critical to ensuring safety and efficiency.

Existing publications confirm the need for an integrated approach to attack modeling. The main gap is the lack of research on attacks on communication channels with repeaters and their impact on the interference immunity of the swarm.To enable emergency remote control and condition monitoring, reliable communications with both long- and short-range UAVs is required.

The aim of this study is to develop a simulation model for analyzing attacks on UAV swarm with a repeater and assessing the impact of attacks. For this purpose, a model of the UAV swarm communication channel was created to simulate Denial of Service (DoS) attacks.

II. Related Works

The article [1] presents an analysis of the types, classifications, charging methods, as well as practical aspects, applications, unsolved problems, safety issues and requirements for the operation

 doi:10.20944/preprints202509.1726.v1

of UAVs. When using drones, there are limitations related to the duration of autonomous flight, range, communication stability, operating time in the air and load capacity. The main objective of the study is to reveal the potential of drones and improve their parameters.

Relay drones are becoming an important element in communication systems due to such advantages as high mobility, adaptability, good visibility and the ability to quickly configure in real time. The article [2] considers the creation of an auxiliary link within the framework of 3GPP standardization and modeling of a communication channel using a repeater on a UAV. The impact of relaying is studied through a circular trajectory model in the NS3 simulator. The results show that in order to meet quality of service requirements, it is more effective to increase the number of relay UAVs than to increase the number of connections on one drone. The use of MIMO technology did not lead to an improvement in data transmission.

The specific features of UAVs require a thorough study of their vulnerabilities. The paper [3] aims to identify the main problems of protecting UAV networks from attacks that exploit their vulnerabilities. The researchers found that significant threats arise not only in individual components of the UAV network, but also in their interaction with other system elements.

When flying long distances or in the presence of obstacles, UAV failures are inevitable. Data transmission via satellite transponders can ensure prompt receipt of information and increase the range of drones. Expanding the coverage area is possible by using satellites as repeaters for transmitting data to the control center. The paper [4] analyzes various adaptive modulation schemes for two typical application scenarios in UAV surveillance systems, where the choice of the optimal transmission scheme depending on the conditions plays an important role.

The paper [5] studies the distribution of resources of satellite and terrestrial feedback channels, as well as radio access. Market conditions are taken into account, where the data transfer rate is optimized using a specialized algorithm. The developed algorithm allows to increase the number of radio channels with the speed over 40 Mbit/s more than twice, and the number of transit channels with the speed over 1.6 Gbit/s more than three times.

In [6], algorithms for constructing shading and loss maps based on modeling of communication channels of UAVs with repeaters located at a fixed height are proposed. With the development of technologies, the use of repeater drones has become a cost-effective way to expand wireless coverage. At a drone flight altitude of 100 meters, the coverage increases by more than 40% compared to a height of 1.5 meters (the average height of a person). The conducted analysis is important for identifying areas with insufficient coverage and assessing the improvements achieved due to retransmission.

Hybrid retransmission network is described [7], combining satellites and UAVs, where repeater drones use coordinated multipoint communication to serve ground users within a single non-orthogonal multiple access cluster. The optimization problem takes into account minimum quality of service requirements, transmission power limitations, and consistent interference suppression to improve energy efficiency. The results show significant improvement in spectral efficiency and reduced outage probability using the proposed approach.

This review article [8] examines privacy issues related to drone standards and regulations. It provides an update on current legislation and the establishment of communications between ground control and the drone. It provides a basic overview of drones, including shortcomings, recent advances, and strategies to address security concerns, attacks, and limitations. It describes areas of research that can be used to create new methods to enhance drone security and privacy.

Attacks on UAV hardware and software systems are increasing, especially attacks on communication systems, coordinate information, attacks on data transmission channels, GPS fraud attacks, authentication attacks, source code vulnerability attacks, and attacks on equipment ports and protocols. This leads to damage such as mission delay, data leakage, mission failure, and loss of prestige. Study [9] discusses the security threats to UAV systems and cyber attacks. Precautions to be taken against threats and attacks are listed. Vulnerability and risk scanning to ensure transmission

 doi:10.20944/preprints202509.1726.v1

security using data encryption methods, data traffic control using a firewall application, and access control are discussed.

Paper [10] is devoted to the issue of data transmission security in the UAV domain. For small UAVs, one of the most widely used protocols is the Micro Air Vehicle Link protocol. This protocol allows for the exchange of small amounts of data between the control station and the UAV. The paper presents selected attacks on UAV data transmission and selected security mechanisms - Bluesnarfing, Bluesmacking, The 'sesame bug' and Blesa. For each attack, an overview of defense mechanisms is given, the purpose of which is to detect the attacks and mitigate their impact. A recommendation is given on how to approach current threats in the UAV domain.

Article [11] summarizes the problems that may arise with UAVs, cyber attacks, and countermeasures used to protect against them. All past cyber attacks on UAVs are described. Message insertion, message manipulation, jamming, and GPS spoofing are the most commonly used cyber attacks against these systems. Securing the electronics and communications in systems using multiple UAVs is of paramount importance to ensure their safety and reliability in military and civilian activities. Over the past decade, many technological methods have been developed to protect UAVs from cyber attacks.

Attacks targeting Inertial Measurement Units (IMUs) in UAVs are addressed in paper [12]. The approach combines a literature review and QuickField simulations with experimental validation using a commercially available 6-degree-of-freedom IMU sensor. A hardware-based electromagnetic shielding solution using mu-metal is proposed to mitigate the impact of IEMI on the sensor performance. The study combines experimental testing with simulations to evaluate the shielding effectiveness under controlled conditions. The measured results show that moderate-power significantly distorts IMU sensor readings, but the proposed shielding method effectively reduces the impact, improving the reliability of the sensor.

A scheme for controlling the safety of UAVs against attacks along the desired trajectory is presented in paper [13]. The scheme includes an attack detector, an attack evaluator, and an Integrated Sliding Mode Security Controller (ISMSC). The malicious interference in the desired trajectory sent by the ground control station to the UAV by attackers is considered. The characteristics of attacks along the desired trajectory are analyzed in the attack simulation. An integrated attack detection scheme based on an unknown input observer and an interval observer is proposed. A robust adaptive observer is used to compensate for the impact of attacks on the control system. An ISMSC with an attack compensation mechanism is proposed. Simulation results are provided to verify the effectiveness of the proposed scheme.

Study [14] examines the assessment methods and application of cybersecurity techniques for UAVs taking into account artificial intelligence (AI)-based tools. The paper analyzes the main threats and attacks against UAVs and AI in UAV systems, identifies key vulnerabilities and limitations of AI use. A classification of countermeasures is developed at both the regulatory and technical levels for both offensive and defensive purposes. Examples of profiling AI quality models for UAV systems are given as a means of AI standardization. The study describes the construction of a quality model and the results of IMECA analysis for the assessment of AI-based onboard systems and UAV defenses used in intelligent mobile systems for humanitarian demining.

A class of cyber attacks targeting a UAV swarm is considered in paper [15]. The focus is on scenarios where an attacker can hack a subset of vehicles in the swarm and make minor changes to their parameters. These hacked vehicles are then able to change the behavior of the entire swarm. The swarm, which includes a mixture of malicious and non-malicious vehicles, is modeled using a system of coupled Partial Differential Equations (PDEs) in a two-dimensional LWR model. A methodology is developed that combines Gaussian Processes (GPs) with 2D PDE model. The method is used to detect the presence of malicious vehicles in the swarm. A Bayesian optimization framework is used to determine the optimal choice of basis and kernel functions that comprise the GP. The simulation results show that this detection architecture successfully detects malicious vehicles as well as their attack mode on traffic.

 doi:10.20944/preprints202509.1726.v1

UAVs are vulnerable to global positioning system (GPS) spoofing attacks, which can confuse their navigation systems and lead to unpredictable catastrophic consequences. To address this problem, a detection method [16] based on stacked ensemble learning is proposed, which combines a convolutional neural network (CNN) and extreme gradient boosting (XGBoost) to detect spoofing signals in GPS data. The stacked model uses XGBoost as the base learner, which is optimized by five-fold cross-validation and uses logistic regression for the final prediction. Magnetic field data is included to improve the robustness of the system and the reliability of detecting GPS spoofing attacks. The experiment showed that the proposed model achieved 99.79% accuracy in detecting GPS spoofing attacks, demonstrating its potential effectiveness in improving the security of UAVs.

UAVs rely on untrusted software components to automate dangerous or critical missions, making them a ripe target for attack. The challenge is to prevent an attacker from compromising the ground control station or the UAV software. An architecture [17] running on a UAV software stack with runtime monitoring and seL4-based software isolation that prevents attackers from exploiting software bugs or stealth attacks is presented. The architecture modernizes legacy UAVs and secures the popular MAVLink protocol, enabling its widespread adoption.

III. Communication Channel Model

The model shown in Figure 1 was developed with the help of NetCracker software environment to simulate attacks on UAV swarm with Repeater. The model includes the following key components: Base Station transmitting Tactical Data and Common Data; intermediate node Repeater, which provides communication between Base Station and Aerial Base Station. The latter provides communication with UAV swarm.

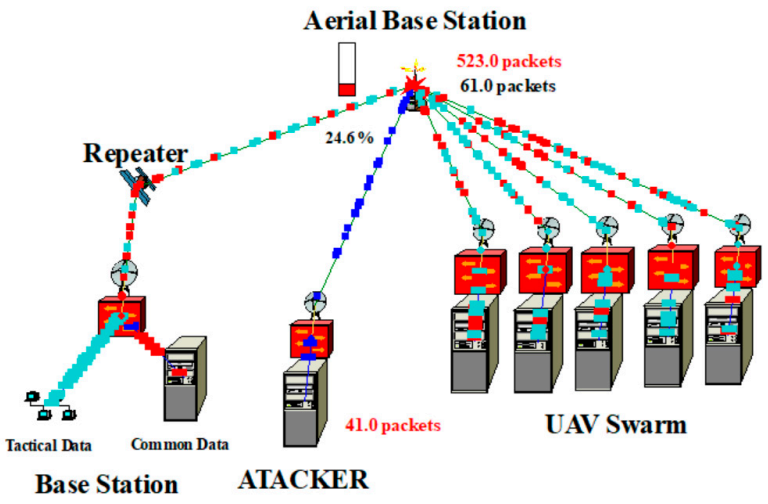

Figure 1. "Base Station – Repeater – Aerial Base Station – UAV Swarm" model.

UAV swarm consists of five UAVs, each of which exchanges data packets with the Base Station. Attacker generates interference that affects the communication between Aerial Base Station, Repeater and UAV swarm. This simulates real electronic warfare scenarios, such as signal jamming. Model parameters are given in Table 1. Repeater is located at a distance of 30 km from Base Station, Aerial Base Station is 10 km from Repeater and UAVs in swarm each on the distance 10 km from Aerial Base Station.

The model is motivated by the need to study the resilience of UAV swarms to attacks in real conditions, where communication is critical for coordination and data transmission. The use of a repeater allows modeling extended communication networks, typical for UAV swarms performing joint missions, such as reconnaissance or monitoring. The inclusion of an attack element reflects real

 doi:10.20944/preprints202509.1726.v1

threats, such as electronic warfare, actively used in modern conflicts (for example, the use of DroneDefender-type rifles to create jamming). The model takes into account various communication parameters (BER, delays, throughput), which allows assessing the impact of attacks on network efficiency.

Model parameters such as channel bandwidth and low BER reflect modern UAV communication standards (e.g. LTE/5G), while latencies meet the requirements of real-time data transmission. The use of Repeater adds realism, as such platforms are increasingly used to provide long-range communications.

The originality of the model is that the integration of UAV swarm with Repeater in the proposed model uniquely combines a swarm with an intermediate repeater, which allows us to study mesh networks in the context of attacks. Most studies focus on direct UAV-Ground or UAV-Satellite communication, while mesh networks with repeaters remain less studied.

Simulating real-time attacks is accomplished by including an attacker to simulate the swarm and is also a novel approach since many UAV communication models do not take into account the impact of interference on swarm communication.

The novelty of the model lies in its integrated approach to attack, as previous studies focused on individual aspects such as communication or recognition without taking attacks into account.

Table 1. "Base Station – Repeater – Aerial Base Station – UAV Swarm" model parameters.

Parameters → **Model elements ↓**	**Bandwidth (Mbps)**	**Length (m)**	**BER (%)**
Base Station			
Tactical Control Data Workgroup	10	-	-
Common Data Server	10	-	-
TCD – Switch link	10	1	0
CD – Switch link	10	1	0
Switch	10	-	-
Switch – Antenna link	44.736	10	0
Antenna	10	-	-
Base Station – Repeater	2.048 - 44.736	30^5	0 – 0.05
Repeater	Packet Latency – 0 s, Packet Fail Chance - 0		
RELAY - Aerial Base Station	10	10^5	0
Aerial Base Station			
Antenna	1000	-	-
Antenna – Server link	44.736	10	0
Server	1000	-	-
Aerial Base Station – UAV in Swarm	10	10^5	0
UAV in Swarm			
Antenna	1000	-	-
Antenna – Switch link	44.736	10	0
Switch	10	-	-
Switch – Server link	10	1	0
Server	10	-	-
ATACKER	10	10^5	0

 doi:10.20944/preprints202509.1726.v1

IV. Attack Simulation

The relevance of our study is related to the increasing number of cyber attacks and electronic attacks on UAVs. For example, interception of drone control in military conflicts, the emergence of new methods of suppressing communications, such as directional interference.

The complexity of control leads to the fact that UAV swarms require stable algorithms for self-organization and adaptation to losses. The loss of a repeater can lead to complete disorganization of the swarm. Insufficient noise immunity of modern communication systems reduces the effectiveness of the swarm in counteraction conditions. It is necessary to develop stable communication protocols and control algorithms.

Modeling attacks allows us to predict the behavior of the swarm in counteraction conditions, optimize control algorithms and increase noise immunity, which is critical for ensuring safety and efficiency.

For the model presented in Figure 1, simulating an attack on UAV Swarm via Aerial Base Station, the choice of the attacker and its characteristics is key to realistic simulation of electronic warfare. To integrate with the model, the Attacker should be connected to the model as a separate node generating interference on the Repeater-UAV Swarm link, with the ability to simulate targeted attacks. Simulating scenarios and testing the attacker with different Time-Between-Transactions (TBT) will allow us to assess the limits of the system's resilience. We will simulate DoS attack aimed at overloading a network or web server in order to make it unavailable to users. "ATTACKER-PC" is one of the tools used in DoS or Distributed Denial of Service (DDoS) attacks to overload the target resource and disable it. The difference between DoS and DDoS attacks is that DoS attacks are carried out on the basis of a single computer, DDoS attacks use two or more hostings. It is more difficult to detect a multi-threaded DDoS attack, since the traffic initially looks organic and does not raise questions from the administrator. DDoS, unlike DoS, allows a hacker to direct significant amounts of traffic to their target.

"ATTACKER-PC" means "attacker's PC" or "intruder's PC". This term can be used in the context of information security to refer to a computer that is used to carry out attacks on other systems.

We will simulate DoS attack aimed at overloading a network or web server in order to make it unavailable to users. DoS attack is a targeted set of actions in which an attacker attacks a computer system or network using a large number of messages to send false traffic and overload the resource. Signs of DoS attack are an increase in the network load and the volume of traffic on connection ports. At the same time, the load on the processor and memory increases sharply, the number of requests to databases or other internal services increases. An attack is considered successful if it achieves the attacker’s goals without completely jamming the network. Quantitative measures of success depend on the context (e.g., application type or system criticality). Packet loss ≥ 1–5% is a success for attacks targeting sensitive applications (streaming video). Even 1–5% loss is enough to cause noticeable lags or interruptions. In the context of UAV control, an attack is considered successful if it achieves packet loss ≥ 2–5%, which is enough to disrupt swarm coordination or delay command transmission.

V. Simulation Results

The model allows to see how packets pass through Repeater and Aerial Base Station. The choice of traffic protocol depends on the nature of data transmission, network architecture, and the role of the attacking node. For regular traffic (without an attack), we select the InterLAN protocol because InterLAN traffic models transmission through several network nodes and interfaces, including those with separate subnets and routing. In our model, the base station and drones are in different subnets, and there is also a relay and air routes. For an attack from ATACKER, we select the LAN Peer-to-Peer protocol because LAN Peer-to-Peer traffic is used for direct attacks at the channel level, local overloads in one Wi-Fi zone or subnet. This protocol is preferable if ATACKER is connected to the

 doi:10.20944/preprints202509.1726.v1

same Wi-Fi segment as drones, operates at the Ethernet frame level, or sends a flood to the local segment.

Data transmission of drones in accordance with the ICAO requirements (ICAO Circular, 2011) is carried out in the form of C3 (Command, Control and Communication) traffic (Figure 1), which consists of the Tactical Control Data (TCD) channel for flight control and the Common Data (CD) channel (for transmitting data from users of cellular networks, information from radars, optical, infrared systems, etc).

Traffic with FTP client profile (File Transfer Protocol) for the Tactical Control Data (TS = 100 Kbit and TBT = 1 s with Const distribution law) and interLAN profile (Local Area Network) for the Common Data (TS and TBT with Const distribution law, TBT = 1 s) was set for our models. Command, control and communication traffic is carried out as two-way communication.

 doi:10.20944/preprints202509.1726.v1

Quantitatively packets loss is estimated as the percentage of packets lost in relation to sent packets. Figure 2 demonstrates the dependences of dropped packets number on the TS parameter for ATTACKER traffic.

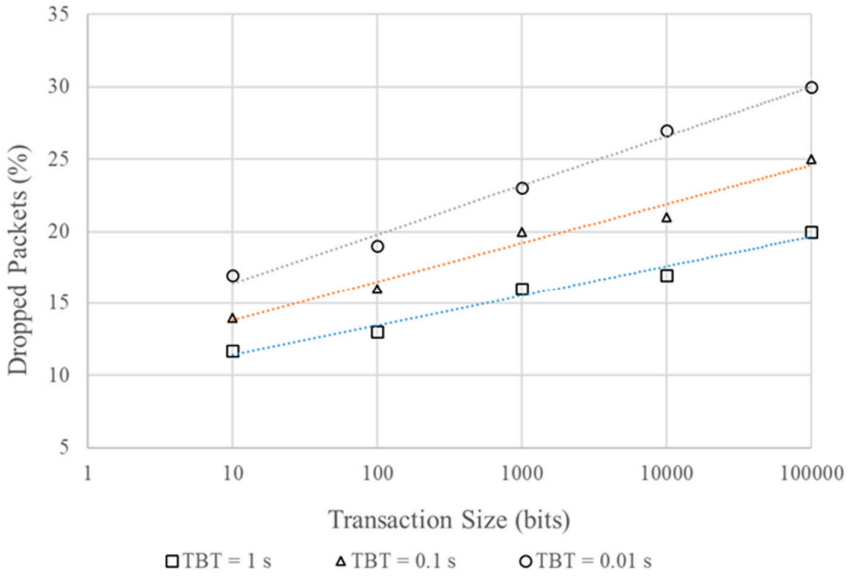

Figure 2. Dependences of dropped packets number on the TS parameter for ATTACKER traffic with different TBT.

Figure 2 shows the packet loss rate at Aerial Base Station as a function of transaction size for three different attacker inter-packet intervals. Aerial Base Station communicates with the UAV swarm via a repeater, and the attacker jams.

TBT = 1 s (squares): Packet loss increases from 10 to about 20% as the transaction size increases from 1 bit to 100,000 bits. The increase is gradual, indicating less attack pressure when the attacker inter-packet intervals are rare.

TBT = 0.1 s (triangles): Losses increase faster, from 15 to 25% over the same transaction size range. This indicates more attack pressure at more frequent intervals.

TBT = 0.01 s (circles): Losses show the fastest increase, from 10 to almost 30% for a transaction size of 100,000 bits. The highest loss is observed at the shortest attacker inter-packet intervals.

The analysis allows us to draw the following conclusions.

Impact of transaction size: Increasing the transaction size leads to an increase in packet loss for all TBT values. This is explained by the fact that larger packets take up more channel resources, making them more vulnerable to interference from an attacking element.

Impact of interpacket time: Decreasing TBT (from 1 s to 0.01 s) significantly increases the level of losses. At TBT = 0.01 s, the attack becomes most intense, leading to channel congestion and loss of up to 30% of packets for large transaction sizes. This indicates a cumulative effect of interference at a high attack frequency.

Vulnerability threshold: For small transaction sizes (1-100 bits), losses remain relatively low (10-15%), regardless of TBT. A significant increase begins at sizes greater than 1000 bits, indicating a critical threshold after which the channel becomes vulnerable to attacks.

Consequences for UAV swarm communication: High packet loss (up to 30% at TBT = 0.01 s) can lead to disruption of swarm coordination, data transmission delays (delays in the model are 0.0–1.2 s) and reduced mission efficiency (e.g. reconnaissance or monitoring). This is especially critical for real time.

Power consumption: Increased losses require retransmissions, which increases the power consumption of UAVs with limited resources, which can reduce battery life.

 doi:10.20944/preprints202509.1726.v1

System reliability: At TBT = 0.01 s and large packet sizes (100,000 bits), the delivery reliability drops to 70%, making the system vulnerable to electronic warfare. This can lead to loss of communication with the ABS or repeater.

Strategic recommendations: Adaptive algorithms should be developed to dynamically adjust the packet size and transmission power. Reducing the transaction size to 1000 bits can reduce losses to 15–20%, even under intense attacks.

VI. Conclusions

This study focuses on addressing the critical issue of interference protection for communication channels in a swarm of UAVs during hostile attacks, a topic of increasing relevance due to the rising threats in both military and civilian domains, such as intelligence gathering, environmental monitoring, and logistics operations. The incorporation of a repeater in the system significantly enhances the operational range and coordination capabilities of the UAV swarm, enabling more effective communication across greater distances. The simulation outcomes revealed that under specific conditions—namely, TBT = 0.01 seconds and a transaction size of 100,000 bits—packet losses escalate to 30%. Such a high packet loss critically impairs the swarm's coordination, leading to operational inefficiencies and a notable increase in energy consumption as the UAVs attempt to compensate for the disruptions. The primary novelty of this research lies in its integration of a repeater within the network architecture and the real-time simulation of attacks, an approach that addresses significant gaps in prior studies by providing a more realistic assessment of swarm behavior under adversarial conditions.

Looking ahead, the findings of this study open several avenues for future research and development. One promising direction is the exploration of advanced interference mitigation techniques, such as adaptive frequency hopping or machine learning-based predictive algorithms, which could dynamically adjust communication protocols in response to detected threats. Additionally, further investigations could focus on optimizing the placement and configuration of repeaters to minimize vulnerabilities while maximizing coverage and reliability. The scalability of the proposed model also warrants examination—future studies could simulate larger swarms with varying numbers of UAVs and repeaters to understand how system performance scales under different attack scenarios. Another critical area of exploration is the energy efficiency of UAV swarms under attack conditions; developing energy-aware routing protocols could help mitigate the increased power consumption observed in this study. Moreover, integrating multi-layered security mechanisms, such as encryption and authentication protocols, could enhance the resilience of communication channels against sophisticated attacks beyond DoS, such as spoofing or jamming. Finally, real-world testing of the simulated model in controlled environments could validate the findings and provide practical insights into the deployment of interference-resistant UAV swarms.

References

1. S. Mohsan, N. Othman, Y. Li, M. Alsharif, and M. Khan, "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends," Intell. Serv. Robot., vol. 16, pp. 109-137, 2023.
2. J. Viana, F. Cercas, A. Correia, R. Dinis, and P. Sebastião, "MIMO relaying UAVs operating in public safety scenarios," Drones, vol. 5, pp. 2-12, 2021.
3. V. Behzadan, "Cyber-physical attacks on UAS networks- challenges and open research problems," arXiv:1702.01251v1 [cs.CR] 4 Feb 2017.
4. R. Xue, M. Zhao, and H. Tang, "Information transmission schemes based on adaptive coded modulation for UAV surveillance systems with satellite relays," IEEE Access, vol. 8, pp. 191355–191364, 2020.
5. Y. Hu, M. Chen, and W. Saad, "Joint access and backhaul resource management in satellite-drone networks: A competitive market approach," IEEE Transactions on Wireless Communications, vol. 19, pp. 3908–3923, 2020.

 doi:10.20944/preprints202509.1726.v1

6. Y. Zhang, T. Arakawa, J. V. Krogmeier, C. R. Anderson, D. J. Love and D. R. Buckmaster, "Large-scale cellular coverage analyses for UAV data relay via channel modeling," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, pp. 1-6, 2020.
7. S. Mirbolouk, M. Valizadeh, A. Chehel, and S. Ali, "Relay selection and power allocation for energy efficiency maximization in Hybrid Satellite-UAV Networks with CoMP-NOMA Transmission," IEEE Transactions on Vehicular Technology, vol. 71, pp. 5087-5100, 2022.
8. A. Ghulam, Z. Saiful, M. Rana, A. Vijanth, and L. Anis, "Comprehensive review of UAV detection, security, and communication advancements to prevent threats," Drones, vol. 6, pp. 284-290, 2022.
9. M. Coşar, "Cyber attacks on unmanned aerial vehicles and cyber security measures," The Eurasia Proceedings of Science Technology Engineering and Mathematics, vol. 21, pp. 258-265, 2022.
10. P. Pekarčík, E. Chovancová, M. Havrilla, and M. Hasin, "Security analysis of attacks on UAV," 2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI).
11. A. Mahalle, S. Khandelwal, A. Dhore, V. Barbudhe, and V. Waghmare, "Cyber attacks on UAV networks: A comprehensive survey," Review of Computer Engineering Research, Conscientia Beam, vol. 11, pp 45-57, 2024.
12. I. Boukabou, N. Kaabouch, and D. Rupanetti, "Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units," Drones, vol. 8, pp. 738-745, 2024.
13. K. Pan, Y. Lyu, F. Yang, et al., "Attack detection and security control for UAVs against attacks on desired trajectory," J Intell Robot Syst, vol. 110, pp. 68-75, 2024.
14. O. Veprytska, and V. Kharchenko, "Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining," IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine.
15. A. Kashyap, A. Chakravarthy, K. Subbarao, D. Casbeer, I. Weintraub, and B. Hencey, "Modeling and Detection of cyber-attacks in UAV swarms using a 2D-LWR model and Gaussian processes," AIAA SCITECH 2024 Forum, 8-12 January 2024, Orlando, FL.
16. T. Ma, X. Zhang, and Z. Miao, "Detection of UAV GPS spoofing attacks using a stacked ensemble method," Drones, vol. 9, pp. 2-15, 2025.
17. A. Amorim, M. Taylor, T. Kann, G. Leavens , W. Harrison , and L. Joneckis, "UAV resilience against stealthy attacks," arXiv:2503.17298v2 [cs.CR] 14 Apr 2025.