*Journal of Artificial Intelligence and Control Systems*

CoSci Press

**Research Article**

# Cognitive Correction of Data Transmission During Attacks on Drone Swarms Which Use Relay

**Volodymyr Kharchenko, Andrii Grekhov*, Vasyl Kondratiuk**

Research Training Center "Aerospace Center", State University "Kyiv Aviation Institute", Kyiv 03058, Ukraine

**Article History:**

Received: 2 July 2025

Revised: 1 August 2025

Accepted: 19 August 2025

Published: 26 December 2025

**Abstract:** Research is devoted to the problem of protecting communication channels for Unmanned Aerial Vehicles (UAVs) swarm using Repeater from interference during attacks. Repeater increases the range of UAVs, but increases vulnerability to attacks. To simulate attacks and cognitive adaptation of channel parameters, an original model "Base Station – Artificial Intelligence System – Attacker – Repeater – UAV Swarm" was created using NetCracker software. Attacker simulates Denial of Service (DoS) attacks. The model allows analyzing the impact of interference on communication, taking into account Average Utilization (AU), data transfer rate (bandwidth), and Bit Error Rate (BER). An algorithm has been developed and code has been provided for implementing adaptation of communication channel parameters in Artificial Intelligence System. The dependencies of AU and BER on time in the process of adapting channel parameters are given. The integration of UAV communication channel with Repeater during imitation of attacks in real time has been implemented, which fills the gaps in existing research. The novelty of this study lies in the interdisciplinary integration that uses radio communication modeling, machine learning methods and UAV-specific network topology to implement cognitive channel adaptation in dynamically changing environments. Proposed approach can be considered pioneering in the context of cognitive correction of drone swarms.

**Keywords:** UAV swarm; DoS attacks; repeater; interference protection

## 1. Introduction

Modern Unmanned Aerial Vehicle (UAV) technology, commonly known as drones, has advanced significantly in recent decades, evolving from highly specialized devices into versatile platforms capable of performing complex missions in a variety of domains [1]. Of particular interest are drone swarms—coordinated groups of UAVs that work together to perform collective reconnaissance, adapt to their environment, and perform missions that require high precision and synchronization [2]. However, implementing such systems faces significant challenges, especially when data are transmitted over wireless links that are susceptible to external influences and attacks. One of the key factors in ensuring the successful operation of a drone swarm is the reliability of the data link, which can be compromised by interference, network congestion, or targeted attacks such as jamming, signal spoofing, or data injection. In this context, cognitive channel correction becomes not only an innovative approach, but also a necessary tool for ensuring the sustainability and efficiency of drone swarms, especially in conditions where a repeater is used to expand the coverage area and improve communication reliability.

The relevance of cognitive correction of the data transmission channel is due to the growing dependence of modern technologies on wireless communication, which, despite its advantages, remains vulnerable to various types of threats [3]. Drone swarms, as highly organized systems, require constant data exchange between individual devices and the central control unit, which makes them especially sensitive to failures in the communication channel. The use of

* Corresponding author: Andrii Grekhov, Research Training Center "Aerospace Center", State University "Kyiv Aviation Institute", Kyiv 03058, Ukraine, grekhovam@gmail.com

repeaters in such systems adds an additional layer of complexity, since signals pass through intermediate nodes, increasing the likelihood of distortions or delays. Attacks on drone swarms, such as electronic jamming or Denial of Service (DoS) attacks, can lead to loss of coordination, collisions, or even complete mission failure. Cognitive correction based on the principles of artificial intelligence and adaptive control allows the system to dynamically analyze the channel state, predict threats and adjust data transmission parameters, which is especially important for drone swarms operating in highly dynamic and uncertain conditions.

One of the key reasons for the relevance of this topic is the rapid growth of drone swarms in military and civilian applications. Military operations increasingly rely on drones for reconnaissance, strikes, and communications in environments where traditional communications may be unavailable or vulnerable. Civilian applications, such as cargo delivery or disaster monitoring, also require reliable communications, especially in remote or hard-to-reach areas, where repeaters play a critical role in providing coverage [4–6]. However, increasing the number of drones in a swarm and the use of repeaters inevitably leads to increased channel congestion, making it more susceptible to attack. Cognitive correction helps minimize these risks by adapting data transmission parameters, such as data rate, signal strength, or frequency, in real time based on an analysis of current conditions.

Another important aspect is the difficulty of ensuring communication security under attack [7,8]. Traditional defense methods such as encryption or the use of fixed frequencies may be insufficient against modern attacks that employ adaptive strategies such as spectrum scanning or targeted jamming. Cognitive systems, on the other hand, are capable of not only detecting channel anomalies but also suggesting optimal solutions to address them, making them particularly valuable for drone swarms. The use of repeaters increases this need, as each additional node represents a potential vulnerability point where an attack can be initiated or amplified. Cognitive correction can include dynamically changing channel parameters, redistributing traffic, optimizing transmission, or even temporarily disabling vulnerable nodes, which significantly increases the resilience of the system.

Historically, wireless technologies have been focused on increasing throughput and reliability, but the emergence of drone swarms has created a need for approaches that take into account not only technical parameters but also cognitive aspects of control. Applying this idea to drone swarms using repeaters involves implementing machine-learning algorithms that analyze channel data such as interference, Bit Error Rate (BER), or Average Utilization (AU) and make decisions about adjusting parameters in real time. For example, if an attack causes BER to increase, the system can automatically reduce the data rate or switch to a less congested frequency, which is especially important for swarms where delays can lead to loss of synchronization.

The relevance of cognitive correction for drone swarms is enhanced by their scalability and autonomy. Unlike single UAVs, swarms consist of dozens or hundreds of devices, each generating and receiving data, which creates a high load (utilization) on the channel. Repeaters used to extend the coverage area or provide communication in difficult terrain conditions add additional points of interaction, which increases the likelihood of interception or distortion of signals. Attacks on such systems can range from simple jamming to complex scenarios such as injection of false commands, which requires the system not only to react but also to predict threats [9–12]. Cognitive correction integrated with repeaters allows for the creation of self-organizing networks, where each node adapts to attack conditions, minimizing the impact on the overall performance of the swarm.

The technical complexity of implementing cognitive correction for drone swarms with repeaters is the need to process large amounts of data in real time. Algorithms must take into account not only the current channel parameters, but also predict future changes based on historical data and attack models. For example, using machine learning methods such as neural networks or regression models can help predict the growth of BER or AU when changing the attacker's parameters. Repeaters, as intermediate nodes, require additional synchronization, which complicates the task, but also provides opportunities for distributed data processing, where each repeater can independently adjust its parameters [13,14].

Cognitive correction of the data transmission channel during attacks on drone swarms using repeaters is a promising direction of research and development. It combines advanced achievements in artificial intelligence, adaptive networks and wireless technologies, offering a solution to one of the key problems of modern UAV systems. This paper aims to study the mechanisms of cognitive correction, their implementation in attack conditions and assess the effectiveness in real scenarios with drone swarms.

In this paper, we propose an original architecture for cognitive correction of communication channel parameters for a UAV swarm using a repeater susceptible to DoS attacks. The main result of the study is the development of the “Base

Station – Artificial Intelligence System – Attacker – Repeater – UAV Swarm" model implemented in the NetCracker environment, which allows real-time modeling of attacks and dynamic channel adaptation based on BER, Average Utilization and throughput indicators. A cognitive correction algorithm has been developed, implemented using linear regression, providing automatic change of data transmission parameters under attack. The program code is described that describes the entire cycle: from modeling the dependence to outputting adaptive tables and graphs of parameter changes over time. The novelty lies in the interdisciplinary integration of radio modeling, artificial intelligence and UAV network topology to increase resilience to external influences. The obtained results can be considered as a step towards the creation of self-organizing and self-adapting unmanned networks that are resistant to overloads and attack effects.

The rest of the paper is organized as follows. Section 2 covers related work. Section 3 presents the architecture and parameters of the model. In Section 4, attack simulation is considered using NetCracker software. Results are discussed in Section 5, and the conclusions are given at the end of the article.

## 2. Related Works

The paper [1] provides an overview of the types, classifications, charging methods, as well as practical aspects, areas of application, unsolved problems, safety issues and requirements for the operation of unmanned aerial vehicles (UAVs). When using drones, there are limitations related to the duration of autonomous flight, communication range, data transmission stability, time in the air and load capacity. The main goal of the study is to reveal the potential of UAVs and improve their characteristics.

Relay drones are becoming a key element of communication systems due to such advantages as high mobility, flexibility, good visibility conditions and the ability to quickly configure in real time. The article [2] considers the organization of an auxiliary communication channel based on 3GPP standards and modeling of a data transmission channel using a UAV-relay. The impact of relaying is analyzed using a circular flight path model in the NS3 environment. The results show that to ensure a given level of service quality, it is more efficient to increase the number of repeater drones than the number of connections to one device. The use of MIMO technology in this case did not improve the data transfer rate.

The specifics of UAV use require a careful study of their vulnerabilities. The work [3] is aimed at identifying key threats to the security of UAV networks that exploit the weaknesses of such systems. It was found that serious risks exist both at the level of individual network components and during their interaction with other elements of the system.

When flying over long distances or in obstacle conditions, UAV failures are inevitable. Data transmission via satellite repeaters allows for prompt receipt of information and increases the range of the devices. Expanding the coverage area is possible through the use of satellites as intermediate nodes for data transmission to control points. The study [4] considers various adaptive modulation schemes for two typical scenarios of UAV use in surveillance systems, where the choice of the optimal option for information transmission plays an important role.

The article [5] analyzes the distribution of resources of satellite and terrestrial feedback channels, as well as radio access. Market conditions are taken into account, under which an increase in data transfer rate is achieved using a specialized algorithm. The developed solution allows more than doubling the number of radio channels with a speed of over 40 Mbit/s and tripling the number of transit channels with a speed of over 1.6 Gbit/s.

The work [6] proposes algorithms for constructing shadowing and signal loss maps based on modeling communication channels between UAVs and repeaters placed at a fixed height. With the development of technology, the use of repeater drones has become an economically viable way to expand the coverage area of wireless networks. It is shown that with a drone flight altitude of 100 meters, the coverage radius increases by more than 40% compared to a height of 1.5 meters (the average height of a person). The analysis allows identifying areas of weak signal and assessing the efficiency of using repeaters.

A hybrid relay network combining satellites and UAVs is described in [7]. In such a system, relay drones use coordinated multipoint transmission to serve ground users within a single cluster with non-orthogonal multiple access. The optimization problem takes into account minimum quality of service requirements, transmission power limitations, and the need to suppress interference to improve energy efficiency. The results show a significant improvement in spectral efficiency and a decrease in the probability of communication failure due to the proposed approach.

A review article [8] is devoted to privacy issues related to regulatory frameworks and standards for UAVs. An analysis of the current legislation is presented, as well as the features of organizing communication between ground control points and a drone. The main characteristics of drones, their disadvantages, modern achievements and approaches to

solving security and attack problems are considered. Promising research areas for developing new methods to improve the security and privacy of UAVs are also highlighted.

The number of attacks on UAV hardware and software systems continues to grow, including attacks on communication channels, navigation systems, data transmission channels, GPS fraud, authentication attacks, source code and hardware port vulnerabilities. Such threats can lead to data leakage, mission failure, delays or loss of trust. The paper [9] examines cyber threats aimed at UAVs and lists measures to prevent them. Methods for ensuring data transmission security are considered, including encryption, traffic control through firewalls and access control.

The number of attacks on UAV hardware and software systems continues to grow, including attacks on communication channels, navigation systems, data transmission channels, GPS fraud, authentication attacks, source code and hardware port vulnerabilities. Such threats can lead to data leakage, mission failure, delays or loss of trust. The paper [9] examines cyber threats aimed at UAVs and lists measures to prevent them. Methods for ensuring data transmission security are considered, including encryption, traffic control through firewalls and access control.

The paper [10] considers data transmission security for small UAVs, in particular, the MAVLink protocol, widely used for exchanging control information between the drone and the control station. An overview of typical attacks is provided - Bluesnarfing, Bluesmacking, "sesame bug" and Blesa, as well as methods for their detection and mitigation. Recommendations are given for protecting UAV systems from current threats.

The work [11] summarizes the known problems of UAV security, examples of cyber attacks and methods of protection against them. Attacks including message insertion and modification, communication jamming and GPS spoofing are described in detail. Ensuring the security of electronics and communications is especially important for multi-agent UAV systems, both in military and civilian applications. Over the past decade, a number of technologies have been developed aimed at protecting such systems from cyber threats.

The article [12] considers attacks on UAV inertial measurement units (IMU). A comprehensive study is presented, including a literature review, communication channel modeling and experimental verification using a commercial 6-axis IMU sensor. As a protective measure, shielding of sensors using a magnetic material - mu-metal is proposed. Tests have shown that the protection significantly reduces the impact of electromagnetic effects on the accuracy of measurements.

The work [13] presents a scheme for increasing the security of UAVs from attacks aimed at changing their trajectory. An architecture is proposed that includes an attack detector, an attack assessment system, and an integrated sliding mode security control (ISMSC). The mechanisms include unknown input observers and interval observers to detect attacks, as well as an adaptive compensator to minimize their impact. The conducted simulation confirms the effectiveness of the proposed approach.

The article [14] considers methods for assessing the cybersecurity of UAVs using artificial intelligence. The main threats, vulnerabilities, and limitations of using AI in unmanned systems are analyzed. A classification of security measures is developed at both the technical and regulatory levels. Examples of AI quality assessment models for UAVs are presented, and the results of applying IMECA risk analysis to assess the security of intelligent mobile platforms used, among other things, for humanitarian demining are presented.

The work [15] considers cyberattacks aimed at UAV swarms, in which an attacker can hack some of the drones and slightly change their parameters, influencing the behavior of the entire group. The swarm is modeled as a system of coupled two-dimensional partial differential equations (LWR model). A method for detecting malicious drones is developed using Gaussian processes (GP) and the Bayesian optimization approach to select the best models and kernels. Simulation shows high efficiency of the proposed architecture in detecting attacking devices and their methods of influence.

UAV vulnerability to GPS spoofing attacks can lead to serious consequences. The study [16] proposed a method for detecting such attacks based on the combination of Convolutional Neural Networks (CNN) and the gradient boosting algorithm (XGBoost). To improve reliability, magnetic field data are included in the system. Tests showed the accuracy of attack detection at 99.79%, which confirms the promise of this approach for improving the safety of UAV navigation.

The reliability of UAV operation largely depends on the security of the software. The paper [17] proposes an architecture for software isolation and execution monitoring based on the seL4 microkernel, designed to prevent exploitation of vulnerabilities and attacks. The architecture ensures secure code execution, modernizes legacy UAV platforms, and strengthens the security of the MAVLink protocol, which is widely used in drone-to-control communications systems.

## 3. Communication Channel Model

The model (Figure 1) was created using NetCracker software (https://www.netcracker.com/) for simulation attacks on UAV swarm with Repeater. The simulation data based on NetCracker was tested and compared with real data, as described in the books [18,19]. The model contain Base Station transmitting and receiving data; Artificial Intelligence System (AIS); Attacker, which generates interference; intermediate node Repeater, which provides communication between Base Station and UAVs in swarm.

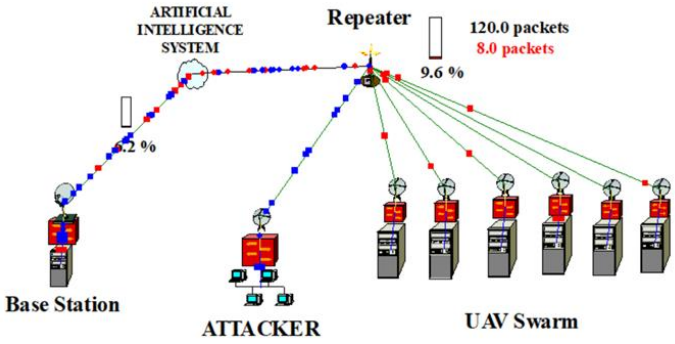


**Figure 1.** "Base Station – Artificial Intelligence System – Attacker – Repeater – UAV Swarm" model

Model parameters are given in Table 1. AIS is located on Repeater and both are at a distance of 30 km from Base Station, UAVs in swarm each on the distance 10 km from Repeater. Attacker is located at a distance of 1–5 km from Repeater.

UAV swarm comprises six unmanned aerial vehicles, each engaging in the exchange of data packets with Base Station. Attacker introduces interference that disrupts the communication link between Base Station, Repeater, and UAV swarm. This setup mimics real-world electronic warfare situations, including scenarios involving signal jamming.

The development of the model and simulation of attacks is motivated by the need to study the resilience of UAV swarm communications to attacks in real-world conditions, where communications are critical for coordination and data transfer. The use of a repeater allows modeling extended communication networks typical of UAV swarms performing joint missions. The inclusion of an attack node reflects real threats actively used in modern conflicts. The model takes into account various communication channel parameters, which allows assessing the impact of attacks on network performance. The use of a repeater reflects a real-world situation, since such platforms are increasingly used to provide long-range communications. The originality of the model lies in the integration of UAV swarm with a repeater containing AIS. Most studies focus on direct UAV-Ground or UAV-Satellite communications, while mesh networks with repeaters remain less studied.

Simulation of real-time attacks is carried out by including an attacker to simulate a swarm and is also a new approach, since many UAV communication models do not take into account the impact of interference on swarm communications. The novelty of the model also lies in its comprehensive approach to attack, as previous studies focused on individual aspects such as communication or recognition without taking attacks into account.

**Table 1**. Model parameters

| **Parameters →<br>Model elements ↓** | **Bandwidth (Mbps)** | **Length (m)** | **BER (%)** |
|---|---|---|---|
| **Base Station** | | | |
| Tactical Control Data Workgroup | 10 | - | - |
| Data Server | 10 | - | - |
| Switch | 10 | - | - |
| Antenna | 10 | - | - |
| Base Station – AIS | 2.048–44.736 | $30^5$ | 0–0.2 |
| **Artificial Intelligence System (AIS)**<br>Packet Latency – 0 s, Packet Fail Chance - 0 | | | |
| AIS – Repeater | 10 | 0 | 0 |
| **Repeater**<br>Packet Latency – 0 s, Packet Fail Chance - 0 | | | |
| **UAV Swarm** | | | |
| UAV Antenna | 1000 | - | - |
| UAV Switch | 10 | - | - |
| UAV Server | 10 | - | - |
| **Attacker** | | | |
| Attacker | 10 | $1000–10^5$ | 0 |

## 4. Simulation of Attacks

The number of cyber-attacks and electronic interference in UAV communication systems is constantly increasing. The interception of drone control during military conflicts or the emergence of new methods for suppressing communications using directional interference highlight this problem. UAV swarms require robust algorithms for self-organization and adaptation to losses due to the complexity of control. A failure in the operation of a repeater can cause complete disorganization of the swarm. Low noise immunity of modern communication systems reduces the effectiveness of the swarm in counteraction conditions. Therefore, it is necessary to develop reliable communication mechanisms and algorithms for adapting transmission control.

Attack modeling allows predicting the swarm behavior under counteraction, optimizing data transmission parameters and, in fact, increasing noise immunity, which is critically important. The model shown in Figure 1 simulates an attack on UAV swarm via Repeater. The choice of the attacking agent and its characteristics plays a key role in creating a realistic scenario. To integrate with the model, the attacker must be connected as a separate node generating interference on the communication line between the repeater and UAV swarm, with the ability to simulate targeted attacks.

In this paper, the impact of the attack is studied by superimposing two traffics (Figure 1): the main traffic (shown in red) from the base station to the drones and the attack traffic (shown in blue) directed through the repeater to the base station.

In the work, scenarios are simulated and the attacker is tested with different Time Between Transactions (TBT) values to assess the limits of the communication channel stability. DoS attack was modeled, aimed at overloading the network or web server to make it unavailable to users.

ATTACKER computer is used in DoS attacks to overload the target resource and disable it. Such an attack is a targeted set of actions in which an attacker affects network by sending a large number of false messages to overload the resource. Signs of DoS attack are an increase in network load (utilization) and an increase in 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 blocking the network. Quantitative success rates depend on the context (e.g., application type or system criticality). An attack on a communication channel is considered successful if it leads to a significant increase in AU, which degrades its throughput and increases the likelihood of delays or packet losses.

## 5. Simulation Results

The model allows analyzing traffic when packets pass through AIS and Repeater. The choice of traffic protocol depends on the nature of data transfer, network architecture, and the role of the attacking node. For non-attack traffic, we choose the InterLAN protocol, since it models transfer through several network nodes and interfaces. For the attack from ATACKER, we choose the LAN Peer-to-Peer protocol, since it is used for direct attacks at the link level, local congestion in one Wi-Fi zone or subnet. This protocol is preferable if ATACKER is connected to the same segment as drones.

### *5.1. Study of Channel Load Dependence on TS for Different Attack Intensities*

Figure 2 shows the dependence of AU on the transaction size for different time intervals of sending attack packets. Key observations are as follows.

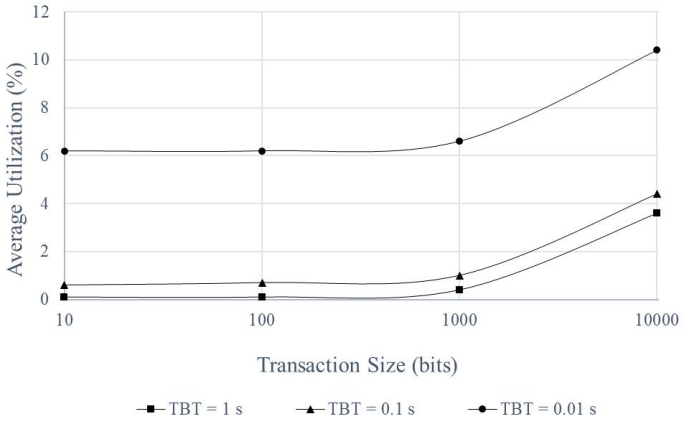


**Figure 2.** Dependences of AU for "BS – AIS" channel on TS for different ATTACKER TBT (TS = 1000 bits) (TBT = 1 s for basic traffic)

*At TBT = 1 s*: AU remains the smallest for all transaction sizes; the attack does not have a serious impact.

*At TBT = 0.1 s*: AU begins to gradually grow with increasing transaction size, especially noticeable after 1000 bits. At TS ≈ 10000 bits, AU reaches about 4%, which can still be considered a moderate impact.

*At TBT = 0.01 s* (aggressive attack): AU is initially

higher even for small transaction sizes (about 5–6%); as TS increases above 1000 bits, AU increases sharply, reaching 10% at TS ≈ 10000 bits; such growth indicates serious channel degradation.

From this, we can draw the following conclusions about the criticality of the attack:

- The shorter the interval between attacking transactions, the stronger the impact of the attack on AU.
- The larger the transaction size, the faster the critical AU is reached.
- AU above 10% can be considered a threshold after which the system begins to experience difficulties.
- The combination of a large TS and a small TBT quickly brings the channel to a critical level of AU, which threatens the stability of the connection between the base station and UAVs.

*5.2. Study of Channel Utilization Dependence on Data Transfer Rate for Different Attack Intensities*

An analysis of AU dependence on channel bandwidth, shown in Figure 3, allows us to draw the following conclusions.

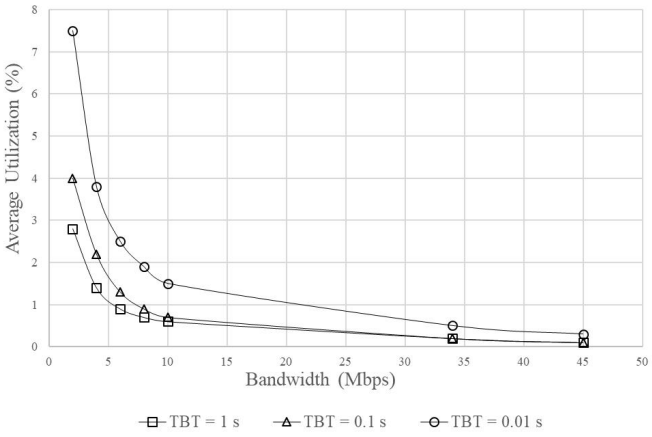


**Figure 3.** Dependences of AU for “BS - AIS” channel on bandwidth for different ATTACKER TBT (TS = 1000 bits) (TS = 10000 bits and TBT = 1 s for basic traffic)

*At TBT = 1 s*: as bandwidth increases, AU tends to decrease, since increasing the channel bandwidth reduces the relative share of the occupied resource; the channel is stable, AU remains low.

*At TBT = 0.1 s*: AU begins to increase, especially noticeable at low bandwidth; the channel begins to fail to cope with the attacking and useful traffic; as bandwidth increases, AU decreases, but the impact of the attack remains noticeable.

*At TBT = 0.01 s* (aggressive attack): AU increases significantly at low and medium bandwidth values; even with increasing bandwidth, the AU level remains high; under low bandwidth conditions, channel overload may occur, leading to errors, delays, and system failures.

The key conclusions are as follows:

The lower the channel bandwidth, the higher the impact of the attack on AU.

- At high attack intensity (low TBT), even a significant increase in channel bandwidth may not ensure stability.
- An increase in AU over 10–15% in a channel is critical, as it can lead to a slowdown in command processing, packet loss, and loss of control over a swarm of drones.

Practical recommendations:

- The minimum required bandwidth should provide AU no higher than 10% even under attack.
- It is necessary to introduce adaptive bandwidth increase or alternative communication routes when attacks are detected.

It is necessary to use mechanisms for packet prioritization in AIS and filtering suspicious traffic to protect critical channels.

*5.3. Study of Channel Utilization Dependence on BER for Different Attack Intensities*

The BER vs. AU dependences for different values of the attacker's TBT are shown in Figure 4. The analysis revealed the following trends.

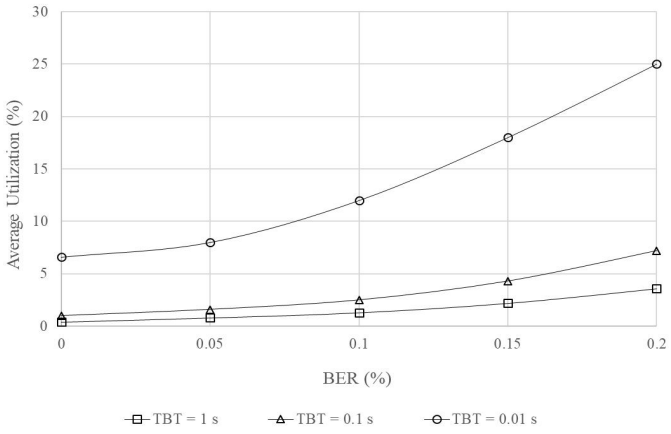


**Figure 4.** Dependences of BER on AU for “BS - AIS” channel for different ATTACKER TBT (TS = 1000 bits) (TS = 1000 bits and TBT = 1 s for basic traffic)

There is an increase in AU with increasing BER: for all TBTs, AU increases with BER, but the growth rate depends on TBT. The smaller the TBT, the faster the AU increases.

*At BER = 0%*: AU is minimal (0.4% for 1 s, 1% for 0.1 s, 6.6% for 0.01 s), which reflects the basic load without errors.

*At BER = 0.2%*: AU reaches 3.6% (1 s), 7.2% (0.1 s), and 25% (0.01 s), showing exponential growth at lower TBT.

Impact of TBT:

*TBT = 1 s*: AU grows slowly (from 0.4% to 3.6% for BER from 0% to 0.2%), which indicates a low attack intensity.

*TBT = 0.1s*: AU increases faster (from 1% to 7.2%), reflecting a moderate attack intensity.

*TBT = 0.01s*: AU increases most sharply (from 6.6% to 25%), signaling a high attack intensity.

General conclusions:

The attack with TBT = 0.01 s is the most dangerous due to the sharp increase in AU, making the channel vulnerable already at BER = 0.1% (AU = 12%).

To ensure swarm stability, it is necessary to maintain AU below 10–12%, which requires either increasing the bandwidth or using cognitive correction to adapt the channel parameters.

The most dangerous scenario occurs at TBT = 0.01 s and BER > 0.15% (AU > 18%), where swarm coordination becomes impossible.

## 6. Theoretical Foundations for Cognitive Correction

To implement cognitive correction of communication parameters in UAV swarm systems under DoS attacks, we use one of the simplest models of Artificial Intelligence (AI)—linear regression. Despite its simplicity, linear regression effectively approximates the relationship between key variables in communication channels, allowing prediction and real-time adaptation of transmission parameters such as BER and AU.

### *6.1. Alternative Artificial Intelligence Methods for Cognitive Parameter Adaptation*

In addition to linear regression, several other AI techniques can be applied to the problem of cognitive adaptation of UAV communication parameters under adversarial conditions such as DoS attacks. These methods aim to predict, adapt, and optimize communication performance metrics.

6.1.1. Candidate AI Methods

(1) Decision Trees and Random Forests (RF):

These non-linear models construct a tree-like structure of decision rules based on input features. Random Forests aggregate multiple decision trees to reduce variance and improve robustness. They are well suited for modeling interactions between TBT, BER, and AU.

(2) Support Vector Machines (SVM):

SVMs are effective in high-dimensional spaces and can model complex relationships through kernel functions. They are generally used for classification or regression tasks but require careful kernel tuning.

(3) Artificial Neural Networks (ANN):

Multi-layer feedforward neural networks can learn highly non-linear mappings between AU, BER, and TBT. ANNs require large datasets and longer training times but are flexible and powerful.

(4) K-Nearest Neighbors (KNN):

A non-parametric method that predicts values based on the closest observed samples. Although simple and interpretable, it scales poorly with data volume and dimensionality.

(5) Gaussian Process Regression (GPR):

A Bayesian method that provides both a mean prediction and a confidence interval. GPR is highly accurate for small datasets but becomes computationally intensive with larger samples.

**Table 2.** Comparative Evaluation of AI Methods

| Method | Complexity | Training Time | Interpretability | Accuracy | Data Requirements | Suitable for UAV Systems |
|---|---|---|---|---|---|---|
| Linear Regression | Very Low | Very Fast | High | Moderate | Low | ✓ Yes (embedded-friendly) |
| Decision Trees / RF | Medium | Fast | Moderate | High | Medium | ✓ Yes |
| SVM | High | Moderate | Moderate | High | Medium | Possibly (depends on kernel |

| | | | | | | |
|---|---|---|---|---|---|---|
| ANN (MLP) | High | Long | Low | Very High | High | ✗ Not optimal for real-time |
| KNN | Medium | None | High | Moderate | Medium | Limited scalability |
| GPR | Very High | Long | High | Very High | Low | ✗ Not scalable for swarms |

As shown in Table 2, linear regression offers key advantages in embedded or constrained UAV platforms due to its: low computational cost, suitable for real-time systems; interpretability, enabling direct analysis of relationships between inputs and outputs; low data requirements, since polynomial-approximated data can bootstrap the model.

6.1.2. Novelty and Scientific Contribution

A unique aspect of the present study is the generation of synthetic training data based on analytically derived polynomial dependencies between BER and AU for various TBT values. This approach is distinct from standard machine learning workflows, where empirical data are collected through direct measurements or simulations.

To our knowledge, no prior publications have systematically used analytical polynomial models to generate extended datasets for training AI-based predictors in the context of UAV communication resilience under DoS attack conditions. Most related works rely on pure simulation data [e.g., NS-3, OMNeT++], reinforcement learning applied to routing or frequency selection, ANN approaches trained on large experimental datasets.

Thus, the current method can be considered a *pioneering hybrid technique*, combining:

- Analytical modeling (via polynomial approximation),
- Data augmentation to overcome sparse real-world training data,
- Lightweight AI algorithms (linear regression) for real-time inference and adaptive response.

This hybrid AI-modeling methodology provides a scalable and explainable framework for UAV swarm protection under electronic warfare conditions.

The integration of synthetic data obtained from polynomial approximations followed by adaptation of transmission parameters in real time (as described in this paper) has not been widely documented. Such an approach can be considered pioneering in the context of cognitive correction of drone swarms, especially considering the use of repeaters and DoS attacks, which distinguishes it from traditional methods.

*6.2. Theoretical Basis of Linear Regression*

Let us consider cognitive correction of data transmission parameters during attacks on drone swarms using a repeater. The task is to create and train a model using simple artificial intelligence methods based on the dependencies between BER and AU at different TBT values. Adaptation of parameters and cognitive correction of data transmission will be carried out, including changing the BER and tracking a given AU threshold. The linear regression method, as one of the basic approaches in the field of artificial intelligence, is chosen due to its simplicity and efficiency for modeling linear dependencies between variables, which makes it suitable for the initial analysis of complex systems such as drone swarms. Linear regression assumes that the dependent variable y (in this case, AU) can be represented as a linear combination of independent variables x (BER and TBT) with the addition of a random error ϵ:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \epsilon, \qquad (1)$$

where $\beta_0$ is the intercept, $\beta_1$ and $\beta_2$ are the regression coefficients for $x_1$ and $x_2$, respectively, and ϵ is a random error with zero expectation and constant variance.

The learning objective is to minimize the sum of squared errors between the observed and predicted values, which is achieved using the least squares method. The optimization problem is formulated as:

$$\min_{\beta_0,\beta_0,\beta_2} \sum_{i=1}^{n} \left(y_i - (\beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2})\right)^2, \qquad (2)$$

where $n$ is the number of observations, $y$ is the observed AU value, $x_{i1}$ is BER value, $x_{i2}$ is TBT value.

The curves in Figure 4 can be approximated by second-degree polynomials with the approximation reliability value

$AU_1 = 68.6 \times BER^2 + 1.9 \times BER + 0.4$, for TBT = 1 s,
$AU_2 = 157.1 \times BER^2 - 1.2 \times BER + 1.1$, for TBT = 0.1 s,
$AU_3 = 377.1 \times BER^2 + 18.2 \times BER + 6.4$, for TBT = 0.01 s.

To train the linear regression model, we create a data array using $AU_1$, $AU_2$, $AU_3$ dependencies with BER step of 0.05%. Based on the created data array, we train a linear regression

model to be able to predict BER for given AU and TBT. The linear regression model is considered as a basic example of artificial intelligence. The trained model is used to predict BER at AU = 12% and TBT = 0.01 s (predicted BER = 0.11%). The BER, AU, and TBT values are printed out, which is used to check the quality of the model.

We use the trained model to adapt the transmission parameters as follows (corresponding block-diagram is given in Appendix A):

- data are transmitted starting from AU = 0%, increasing in 0.025% increments every minute of transmission;
- the transmission process is displayed on AU (t) dependency graph;
- as soon as the value of the parameter AU reaches the value AU = 4%, the value of BER (%), is printed indicating that the adaptation threshold has been reached;
- after this, AU is decreased by 3% and the transmission process is continued with a step of 0.025% every minute of transmission, displaying on the same graph the dependencies AU (t);
- after reaching the value AU = 4% three times, the data transmission is stopped, and the cognitive correction of the data transmission parameters is displayed in Figures 5 and 6 of the dependencies AU (t) and BER (t).

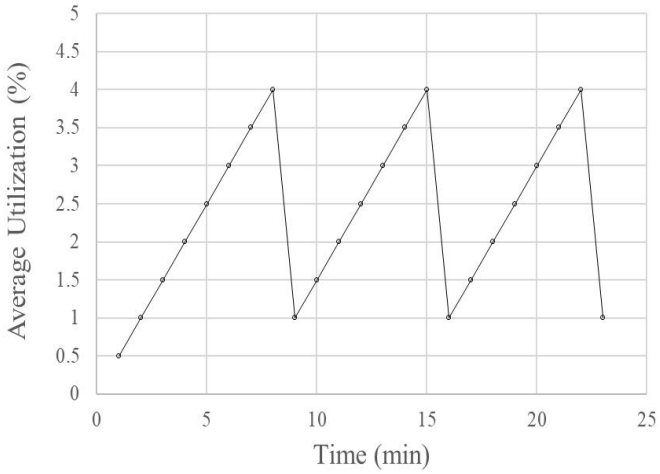


**Figure 5**. Graph of the dependence AU(t)

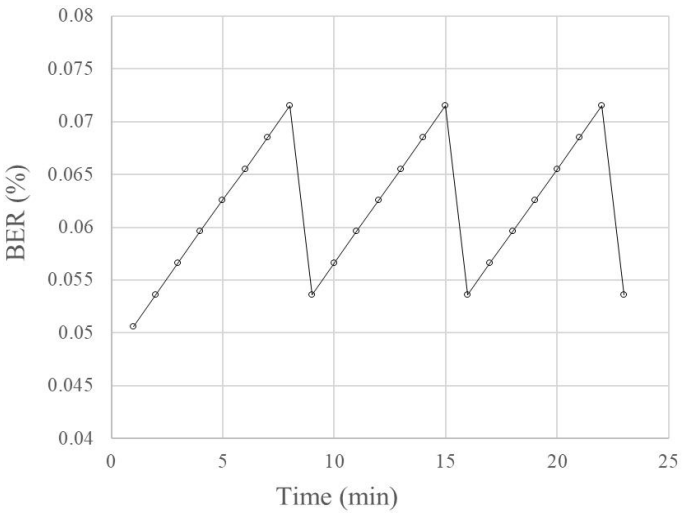


**Figure 6**. Graph of the dependence BER(t)

## 7. Conclusions

This research presents a comprehensive approach to enhancing the resilience of UAV swarm communication channels that utilize Repeater, which, while extending operational range, introduces additional vulnerability to intentional interference. A simulation model "Base Station – Artificial Intelligence System – Attacker – Repeater – UAV Swarm" was developed using NetCracker to replicate real-world conditions, including DoS attacks and dynamic adaptation of channel parameters.

The results demonstrate that cognitive adaptation mechanisms implemented within Artificial Intelligence System significantly improve communication stability under attack conditions. The developed algorithm effectively adjusts channel parameters in real time, reducing average utilization and bit error rate, thus maintaining reliable data exchange within the swarm.

It was shown that under aggressive DoS attacks with reduced intervals between attacker transmissions, AU and BER increase sharply, leading to potential communication degradation. However, with the proposed cognitive correction, the system dynamically mitigates the negative impact, restoring acceptable levels of channel load and reliability.

The novelty of this work lies in the practical integration of UAV-specific communication modeling, interference simulation, and machine learning-based cognitive control. The approach provides a real-time adaptive solution for maintaining UAV swarm coordination in contested environments.

Linear regression remains the optimal choice for the initial stage of research due to its simplicity and efficiency, and the proposed data-augmented approach may represent a novel

contribution to the field.

Future work will focus on expanding the set of attack scenarios, integrating mobility models for UAVs, and testing the approach in more complex multi-hop topologies.

**Statements & Declarations**

**Funding:** The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

**Competing Interests:** The authors have no relevant financial or non-financial interests to disclose.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Author Contributions:** Volodymyr Kharchenko – V.Kh., Andrii Grekhov – A.G., Vasyl Kondratiuk – V.K. Conceptualization, A.G. and V.Kh.; methodology, A.G.; validation, A.G., V.Kh. and V.K.; investigation, A.G.; resources, V.Kh. and V.K.; writing—original draft preparation, A.G.; writing—review and editing, V.K.; supervision, V.Kh.; project administration, V.K. All authors have read and agreed to the published version of the manuscript.

**Ethics Approval:** Not applicable.

**Data Availability Statement:** All data generated and analyzed during this study are included in this article. The datasets generated during the current study are available from the corresponding author on request.

**References**

[1] Mohsan, S.; Othman, N.; Li, Y.; Alsharif, M.; Khan, M. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot*. **2023**, *16*, 109–137.

[2] Viana, J.; Cercas, F.; Correia, A.; Dinis, R.; Sebastião, P. MIMO relaying UAVs operating in public safety scenarios. *Drones* **2021**, *5*, 2–12.

[3] Behzadan, V. Cyber-physical attacks on UAS networks - challenges and open research problems. *arXiv:1702.01251v1 [cs.CR]* **2017**.

[4] Xue, R.; Zhao, M.; Tang, H. Information transmission schemes based on adaptive coded modulation for UAV surveillance systems with satellite relays. *IEEE Access* **2020**, *8*, 191355–191364.

[5] Hu, Y.; Chen, M.; Saad, W. Joint access and backhaul resource management in satellite-drone networks: A competitive market approach. *IEEE Transactions on Wireless Communications* **2020**, *19*, 3908–3923.

[6] Zhang, Y.; Arakawa, T.; Krogmeier, J. V.; Anderson, C. R.; Love, D. J.; Buckmaster, D. R. Large-scale cellular coverage analyses for UAV data relay via channel modeling. *ICC 2020 - 2020 IEEE Int. Conf. Commun. (ICC)* **2020**, *1*, 1–6.

[7] Mirbolouk, S.; Valizadeh, M.; Chehel, A.; Ali, S. Relay selection and power allocation for energy efficiency maximization in Hybrid Satellite-UAV Networks with CoMP-NOMA Transmission. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5087–5100.

[8] Ghulam, A.; Saiful, Z.; Rana, M.; Vijanth, A.; Anis, L. Comprehensive review of UAV detection, security, and communication advancements to prevent threats. *Drones* **2022**, *6*, 284–290.

[9] Coşar, M. Cyber attacks on unmanned aerial vehicles and cyber security measures. *Eurasia Proc. Sci. Technol. Eng. Math*. **2022**, *21*, 258–265.

[10] Pekarčík, P.; Chovancová, E.; Havrilla, M.; Hasin, M. Security analysis of attacks on UAV. *2023 IEEE 21st World Symp. Appl. Mach. Intell. Inform.* (SAMI).

[11] Mahalle, A.; Khandelwal, S.; Dhore, A.; Barbudhe, V.; Waghmare, V. Cyber attacks on UAV networks: A comprehensive survey. *Rev. Comput. Eng. Res.* **2024**, *11*, 45–57.

[12] Boukabou, I.; Kaabouch, N.; Rupanetti, D. Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units. *Drones* **2024**, *8*, 738–745.

[13] Pan, K.; Lyu, Y.; Yang, F.; Tan, Z.; Pan, Q. Attack detection and security control for UAVs against attacks on desired trajectory. *J. Intell. Robot. Syst.* **2024**, *110*, 68–75.

[14] Veprytska, O.; Kharchenko, V. Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining. In Proceedings of the 5th International Workshop on Intelligent Information Technologies and Systems for Information Security (IntelITSIS), Khmelnytskyi, Ukraine, 28 March 2024.

[15] Kashyap, A.; Chakravarthy, A.; Subbarao, K.; Casbeer, D.; Weintraub, I.; Hencey, B. Modeling and Detection of cyber-attacks in UAV swarms using a 2D-LWR model and Gaussian processes. *AIAA SCITECH 2024 Forum* **2024**.

[16] Ma, T.; Zhang, X.; Miao, Z. Detection of UAV GPS spoofing attacks using a stacked ensemble method.

*Drones* **2025**, *9*, 2–15.

[17] Amorim, A.; Taylor, M.; Kann, T.; Leavens, G.; Harrison, W.; Joneckis, L. UAV resilience against stealthy attacks. *arXiv:2503.17298v2 [cs.CR]* **2025**.

[18] Grekhov, A. Recent advances in satellite aeronautical communications modeling. *IGI Global* **2019**.

[19] Grekhov, A. Modeling of aircraft and RPAS data transmission via satellites. In *Research anthology on reliability and safety in aviation systems, spacecraft, and air transport*. IGI Global: Hershey, PA, USA, 2021; pp. 187–236.