Article

AI-Based Detection of Jamming Attacks In 6G Drone Networks

Sergio Cibecchini [1,†,‡], Francesco Chiti [2,‡] and Firstname Lastname [2,*]

[1] Affiliation 1; e-mail@e-mail.com
[2] Affiliation 2; e-mail@e-mail.com
[*] Correspondence: sergio.cibecchini@gmail.com; Tel.: (optional; include country code; if there are multiple corresponding authors, add author initials) +xx-xxxx-xxx-xxxx (F.L.)
[†] Current address: Affiliation.
[‡] These authors contributed equally to this work.

Abstract: A single paragraph of about 200 words maximum. For research articles, abstracts should give a pertinent overview of the work. We strongly encourage authors to use the following style of structured abstracts, but without headings: (1) Background: place the question addressed in a broad context and highlight the purpose of the study; (2) Methods: describe briefly the main methods or treatments applied; (3) Results: summarize the article's main findings; (4) Conclusions: indicate the main conclusions or interpretations. The abstract should be an objective representation of the article, it must not contain results which are not presented and substantiated in the main text and should not exaggerate the main conclusions.

Keywords: keyword 1; keyword 2; keyword 3 (List three to ten pertinent keywords specific to the article; yet reasonably common within the subject discipline.)

Citation: Cibecchini, S.; Chiti, F.; Lastname, F. AI-Based Detection of Jamming Attacks in 6G Drone Networks. *Future Internet* **2024**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

1. Introduction

The shift from 4G to 5G has been a generational leap has revolutionized connectivity around the world. Despite 5G being still in its early adoption rate at the time of writing [1], the research community is already working on the next generation of wireless communication technologies, 6G. 6G technology is expected to enable a wide variety of new use cases, thanks to the increases in both data rates and latency but this in turn will also bring forth new security challenges, specific to those applications.

One of the main differences between 5G and 6G technology will be the focus of the 6G standard in regards to AI integration. While Software Defined Networks (SDN) have played a key role in improving the efficiency and security of 5G networks, 6G is expected to take this a step further, by integrating artificial intelligence and machine learning directly into the network. This is what the authors of [2] define as the shift from *Softwarization* to *Intelligentization*.

AI integration in 6G networks will greatly strengthen the security of the network against security threats. By leveraging Diagnostic Analytics, a collection of insights into the status of the networks, security teams will be able to train specific AI models to detect and respond to security threats in real-time.

In this paper we will focus on a specific aspect of the security of 6G networks, namely we will provide a machine learning based approach for the detection of jamming attacks in networks of drones.

The paper is divided in 5 sections:

1. **Topic overview:** In this section we will discuss how drones can benefit from integration in 6G network, analyze jamming attacks, their types, mitigation and detection. Finally we will discuss the advantages of an edge AI approach for jamming detection.
2. **Materials and methods:** In this section we will define the scenario that we decided to analyze as well as the dataset, algorithm and evaluation metrics we chose for our tests.

3. **Numerical Results:** In this section we will present the testing methodology as well as the numerical results that we obtained.
4. **Discussion:** In this section we will discuss the results obtained in the previous section and highlight notable trends.
5. **Conclusions:** In this section we will summarize the results and discuss possible future research directions.

2. Related Works

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

3. Topic Overview

3.1. Drones in 6G Networks

Drones, also known as Unmanned Aerial Vehicles (UAVs) are defined as *all aircraft designed to fly without a pilot on board* [3]. This technology has experienced rapid growth in recent years and is expected to keep growing in both the consumer sector as well as the commercial and military sectors [4].

In report 22.886 [5] 3GPP, the organ responsible for the development and maintenance of the 5G standard, identifies some of the envisioned use cases for 5G V2X (Vehicle-to-Everything) communication services. Among these use cases, the report identifies vehicle platooning, advanced and remote driving end extended situational awareness as some of the main benefits of V2V communication. All these use cases can be leveraged by a 6G drone network to achieve fast and reliable drone-to-drone communication, that, with the integration of artificial intelligence would allow the drones to act autonomously in a coordinated manner.

This would prove useful in a variety of fields: from autonomous soil and crop health assessment as well as irrigation in agriculture, delivery of life saving supplies and locating of survivors in disaster response, in the delivery sector as a more eco friendly alternative to traditional delivery options and possibly in the mobility sector as a complement to traditional taxis and public transportation [6].

The effectiveness of drones in the military sector is widely recognized, both for high and low end models. For example, in the Ukraine war even cheap FPV drones mounted with explosives were successfully used to destroy much more expensive equipment [7].

Security against Jamming attacks is crucial in all these applications, especially in a safety critical environment.

3.2. Understanding Jamming Attacks

Jamming attacks are a type of Denial of Service (DoS) attack that aims at disrupting the communication between two or more devices. This is achieved by transmitting a powerful signal on the same frequency as the one used by the devices to communicate. If the jamming signal is strong enough, it is able to overwhelm the legitimate signal, effectively blocking the communication between the devices [6]. Since the ability to communicate is affected, Jamming attacks falls under the umbrella of attacks that target the *Availability* of the service in the CIA triad classification [8]. Jamming attacks can be classified into 5 main categories, based on the attack pattern of the jammer:

- **Constant Jamming:** The jammer continuously transmits a strong signal on the same frequency as the devices it wants to disrupt.
- **Periodic Jamming:** The jammer simply transmits a strong signal on the same frequency as the devices it wants to disrupt for a certain period of time t_a, then stops transmitting for another period of time t_b. This type of jamming attack is particularly effective against devices that are not able to change their frequency and has the ability to disrupt the transmission of a sequence of consecutive packets. [9]
- **Random Jamming:** In random jamming, the jammer is active at random intervals, giving each transmitted packet a probability p of being jammed [9].
- **Reactive Jamming:** A reactive jammer starts transmitting its jamming signal only when it senses energy in the communication channel, indicating that a legitimate transmission is taking place. This type of jamming attack is more power efficient compared to other operation types, as it only transmits its signal when it is needed[10].
- **Smart Jamming:** A smart jammer is a more sophisticated type of jammer that is able to adapt its jamming signal to maximize the disruption of the communication between the devices. Smart jammers are able to modify their attack pattern based on the transmission specifics of the devices they are targeting and are able to adapt to changes in the communication channel[11].

An effective Jamming detection AI model should achieve a high detection score against all the different types of jamming attacks.

3.3. Jamming attacks against drone networks

Jamming attacks are particularly effective against drone networks, as drones usually rely on external input to navigate and operate correctly. If a jammer were able to completely block the communication between the drone and the base station, the drone would be left without any indication on how to behave and would need to activate an internal failsafe mechanism. This usually comes in the form of either a return to base procedure, a landing procedure or a hover in place procedure. All of these procedures leave the drone in a vulnerable position, as a bad actor could potentially capture the drone and use it for malicious purposes. This is especially true when jamming attacks are used in combination with other types of attacks, such as spoofing attacks.

One real world example of this is the capture of an American drone by Iran in 2011. In December 2011 a Lockheed Martin RQ-170 Sentinel drone operated by the United States Air Force was flying over Iran when its operators lost control of the vehicle. The US government initially claimed that the drone had crashed due to a technical malfunction, but later reports revealed that the drone had been captured by the Iranian military. Iranian electronic warfare specialists claimed to have brought it down using a Jamming attack, that forced the drone into a return to base procedure, in combination with a GPS spoofing attack, that made the drone land into a designated area [12]. After successfully capturing the drone, the Iranian government managed to reverse-engineer the drone and produce a working replica, which was then used in their military operations [13].

3.4. Centralized vs Edge approach for Jamming detection

When presenting a machine learning based approach in an IoT setting, the question of where the AI model should be placed often arises. By their nature, IoT devices, and in turn drones, are usually resource constrained, both in terms of computational power but also in terms of internal storage and battery capacity [14]. This means that complex AI models and algorithms are usually not feasible to be run on the device itself. A centralized approach offloads the computational burden to a central server, that returns the results of the AI model to the device. While this approach might be feasible in some cases, in a real-time situation such as a jamming attack, the latency introduced by the communication with the central server means less time to react to the attack. Also, as jamming attacks degrade or sometimes completely block the communication between the device and the base station, a centralized approach might not be feasible in this case. An lightweight edge approach on the other hand, while not as powerful as a centralized approach, would to provide real-time results to the device and would be able to operate even when the communication is disrupted.

3.5. Detection and Mitigation of Jamming Attacks

When attempting to mitigate jamming attacks, the first step is always to detect that an attack is taking place. This can be done by monitoring the communication channel for signs of jamming. The most common approaches involve the analysis of metrics such as the Signal to Noise Ration (SNR), the Received Signal Strength Indicator (RSSI) and the Packet Delivery Ratio (PDR) [15]. The most simple way to detect jamming attacks is to set a static threshold for these metrics and trigger an alarm when the threshold is crossed. While this approach easy to implement and might be effective in some cases, it is not able to adapt to changes in the communication channel and might be prone to false positives. Implementing a machine learning based approach for jamming detection would allow the system to adapt to the changes in the communication channel and would be able to provide a more accurate detection of jamming attacks [9]. This is especially useful in mobile scenarios like drone networks, where the environment is constantly changing and the signal strength can vary greatly.

Once an attack is successfully detected, state of the art jamming mitigation techniques, like Direct Sequence Spread Spectrum (DSSS), Frequency Hopping (FHSS) and advanced signal processing techniques can be put in place to mitigate the effects of the attack.

4. Materials and Methods

Materials and Methods should be described with sufficient details to allow others to replicate and build on published results. Please note that publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication.

Interventionary studies involving animals or humans, and other studies require ethical approval must list the authority that provided approval and the corresponding ethical approval code.

> This is an example of a quote.

5. Results

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

5.1. Subsection

5.1.1. Subsubsection

The text continues here.

5.2. Figures, Tables and Schemes

All figures and tables should be cited in the main text as Figure 1, Table 1, etc.

Figure 1. This is a figure. Schemes follow the same formatting. If there are multiple panels, they should be listed as: (**a**) Description of what is contained in the first panel. (**b**) Description of what is contained in the second panel. Figures should be placed in the main text near to the first time they are cited. A caption on a single line should be centered.

Table 1. This is a table caption. Tables should be placed in the main text near to the first time they are cited.

Title 1	**Title 2**	**Title 3**
Entry 1	Data	Data
Entry 2	Data	Data [1]

[1] Tables may have a footer.

The text continues here (Figure 2 and Table 2).

Figure 2. This is a wide figure.

Table 2. This is a wide table.

Title 1	**Title 2**	**Title 3**	**Title 4**
Entry 1 *	Data Data Data	Data Data Data	Data Data Data
Entry 2	Data Data Data	Data Data Data	Data Data Data
Entry 3	Data Data Data	Data Data Data	Data Data Data
Entry 4	Data Data Data	Data Data Data	Data Data Data

* Tables may have a footer.

Text.

Text.

5.3. Formatting of Mathematical Components

This is the example 1 of equation:

$$a = 1, \tag{1}$$

the text following an equation need not be a new paragraph. Please punctuate equations as regular text.

This is the example 2 of equation:

$$a = b + c + d + e + f + g + h + i + j + k + l + m + n + o + p + q + r + s + t + u + v + w + x + y + z \tag{2}$$

Please punctuate equations as regular text. Theorem-type environments (including propositions, lemmas, corollaries etc.) can be formatted as follows:

Theorem 1. *Example text of a theorem.*

The text continues here. Proofs must be formatted as follows:

Proof of Theorem 1. Text of the proof. Note that the phrase "of Theorem 1" is optional if it is clear which theorem is being referred to. □

The text continues here.

6. Discussion

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

7. Conclusions

This section is not mandatory, but can be added to the manuscript if the discussion is unusually long or complex.

8. Patents

This section is not mandatory, but may be added if there are patents resulting from the work reported in this manuscript.

Author Contributions: For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing—original draft preparation, X.X.; writing—review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.", please turn to the CRediT taxonomy for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER grant number XXX." and and "The APC was funded by XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding, any errors may affect your future funding.

Institutional Review Board Statement: In this section, you should add the Institutional Review Board Statement and approval number, if relevant to your study. You might choose to exclude this statement if the study did not require ethical approval. Please note that the Editorial Office might ask you for further information. Please add "The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of NAME OF INSTITUTE (protocol code XXX and date of approval)." for studies involving humans. OR "The animal study protocol was approved by the Institutional Review Board (or Ethics Committee) of NAME OF INSTITUTE (protocol code XXX and date of approval)." for studies involving animals. OR "Ethical review and approval were waived for this study due to REASON (please provide a detailed justification)." OR "Not applicable" for studies not involving humans or animals.

Informed Consent Statement: Any research article describing a study involving humans should contain this statement. Please add "Informed consent was obtained from all subjects involved in the study." OR "Patient consent was waived due to REASON (please provide a detailed justification)." OR "Not applicable" for studies not involving humans. You might also choose to exclude this statement if the study did not involve humans.

Written informed consent for publication must be obtained from participating patients who can be identified (including by the patients themselves). Please state "Written informed consent has been obtained from the patient(s) to publish this paper" if applicable.

Data Availability Statement: We encourage all authors of articles published in MDPI journals to share their research data. In this section, please provide details regarding where data supporting reported results can be found, including links to publicly archived datasets analyzed or generated during the study. Where no new data were created, or where data is unavailable due to privacy or ethical restrictions, a statement is still required. Suggested Data Availability Statements are available in section "MDPI Research Data Policies" at https://www.mdpi.com/ethics.

Acknowledgments: In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: Declare conflicts of interest or state "The authors declare no conflicts of interest." Authors must identify and declare any personal circumstances or interest that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results must be declared in this section. If there is no role, please state "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results".

Abbreviations

The following abbreviations are used in this manuscript:

SDN	Software Defined Networks
UAVs	Unmanned Aerial Vehicles
3GPP	3rd Generation Partnership Project
V2X	Vehicle to Everything
FPV	First Person View
DOS	Denial Of Service
SNR	Signal to Noise Ratio
RSSI	Received Signal Strength Indicator
PDR	Packet Delivery Ratio
CIA	Confidentiality, Integrity, Availability
IoT	Internet of Things
AI	Artificial Intelligence
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	Linear dichroism

Appendix A

Appendix A.1

The appendix is an optional section that can contain details and data supplemental to the main text—for example, explanations of experimental details that would disrupt the flow of the main text but nonetheless remain crucial to understanding and reproducing the research shown; figures of replicates for experiments of which representative data are shown in the main text can be added here if brief, or as Supplementary Data. Mathematical proofs of results not central to the paper can be added as an appendix.

Table A1. This is a table caption.

Title 1	Title 2	Title 3
Entry 1	Data	Data
Entry 2	Data	Data

Appendix B

All appendix sections must be cited in the main text. In the appendices, Figures, Tables, etc. should be labeled, starting with "A"—e.g., Figure A1, Figure A2, etc.

References

1. 5G - statistics & facts. Available online: https://www.statista.com/topics/3447/5g/topicOverview (accessed on 13 September 2024).
2. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; AI, B. The Roadmap to 6G: AI Empowered Wireless Networks. *IEEE Communications Magazine* **2019**, *57*, 84–90. https://doi.org/10.1109/MCOM.2019.1900271.
3. Unmanned aircraft (drones). Available online: https://transport.ec.europa.eu/transport-modes/air/aviation-safety/unmanned-aircraft-drones_en (accessed on 13 September 2024).
4. Laricchia, F. Consumer and commercial drones - statistics and facts. Available online: https://www.statista.com/topics/7939/drones/#topicOverview (accessed on 13 September 2024).
5. Sultan, A. Study on enhancement of 3GPP support for 5G V2X services. Tech. Rep. *3GPP*, 2018.
6. Hassija, V.; Kumar, R.; Gupta, H.; Singh, S.; Sharma, P. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials* **2021**, *23*, 2802–2832. https://doi.org/10.1109/COMST.2021.3097916.
7. Rao, A.; Zafra, M.; Hunder, M.; Kiyada, S. How drone combat in Ukraine is changing warfare. Available online: https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/ (accessed on 13 September 2024).
8. Cawthra, J. Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. *NIST Special Publication* **2020**, *1800-26A*.
9. Lyamin, N.; Samuylov, A.; Gaidamaka, Y.; Vinel, A.; Koucheryavy, Y. AI-Based Malicious Network Traffic Detection in VANETs. *IEEE Network* **2018**, *32*, 15–21. https://doi.org/10.1109/MNET.2018.1800074.
10. Boualouache, A.; Engel, T. A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks. *IEEE Communications Surveys and Tutorials* **2023**, *25*, 1128–1172. https://doi.org/10.1109/COMST.2023.3236448.
11. Feng, S.; Haykin, S. Cognitive Risk Control for Anti-Jamming V2V Communications in Autonomous Vehicle Networks. *IEEE Transactions on Vehicular Technology* **2019**, *68*, 9920–9934. https://doi.org/10.1109/TVT.2019.2935999.
12. Owano, N. RQ-170 drone's ambush facts spilled by Iranian engineer. Available online: https://phys.org/news/2011-12-rq-drone-ambush-facts-iranian.html (accessed on 14 September 2024).
13. Gross, J.A.; TOI Staff. Iranian UAV that entered Israeli airspace seems to be American stealth knock-off. Available online: https://www.timesofisrael.com/iranian-uav-that-enteredisraeli-airspace-seems-to-be-american-stealth-knock-off (accessed on 16 May 2024).
14. Chorti, A.; Hollanti, C.; Koorapaty, H.; Poor, H.V. Context-Aware Security for 6G Wireless: The Role of Physical Layer Security. *IEEE Communications Standards Magazine* **2022**, *6*, 102–108. https://doi.org/10.1109/MCOMSTD.0001.2000082.
15. Sciancalepore, S.; Kusters, F.; Abdelhadi, N.K.; Oligeri, G. Jamming Detection in Low-BER Mobile Indoor Scenarios via Deep Learning. *arXiv* **2023**, eprint: 2306.10912. Available online: https://arxiv.org/abs/2306.10912.