Design of Protection Mechanisms for the Internet of Drones

Alisson R. Svaigen[1], Linnyer B. Ruiz[2] (co-advisor), Antonio A. F. Loureiro[1] (advisor)

[1]Computer Science Department
Federal University of Minas Gerais (UFMG) – Belo Horizonte – MG – Brazil

[2]Manna Research Group, State University of Maringá (UEM) – Maringá – PR – Brazil

{alissonsvaigen, loureiro}@ufmg.dcc.br, lbruiz@uem.br

Abstract. *The Internet of Drones (IoD) emerged as a novel mobile network paradigm. IoD is a unique environment with particular characteristics that differ from traditional ones (e.g., drones' mobility and the fast network topology change), demanding compliance with security and privacy requirements. Likewise, IoD can suffer from novel drone-centered threats. The existent protection mechanisms (PMs) may not be adequate for the IoD environment since they may not embrace the IoD characteristics, also facing new threats. Therefore, the main goal of this dissertation is to study the design of PMs for the IoD, considering its particular characteristics. This study reveals a need to enhance current PMs to meet the IoD characteristics since they can not offer the same protection level. Our contributions advance the state-of-the-art on four fronts: new guidelines for IoD security and privacy field; novel location privacy PMs; novel anti-jamming PMs; and new strategies for automatic drone detection.*

1. Introduction

Over the last years, the UAV, also known as "drone", has gained new business interests in different fields, where different companies (e.g., Amazon, Google, and Uber) have been exploring the use of drones as a service (DaaS) [Boccadoro et al. 2021, Bine et al. 2022]. Several reports point out a massive growth of the drone market, resulting in an increase of about U$ 35 billion by 2025 [Tsao et al. 2022]. From a Computer Network point-of-view, the widespread utilization of drone-based technology creates a heterogeneous mobile network environment composed of different drones with different purposes acting as nodes, significantly enhancing Intelligent Transportation Systems (ITS) due to drone's mobility, autonomous operation, and communication capabilities [Boccadoro et al. 2021]. Therefore, the next generation of UAV networks will require a robust, reliable, and interoperable network to accomplish organized and collision-avoidance airspace.

Anticipating this environment, [Gharibi et al. 2016] proposed a layered network architecture named the Internet of Drones (IoD). This network aims to coordinate the access of UAVs to controlled airspace, providing navigation services to drones. Despite this definition, IoD can also refer to broad-scale UAV networks, ranging from swarm-based to an interoperable environment, integrating different network infrastructures. IoD has particular characteristics compared to ground mobile networks, such as Vehicular Ad hoc Networks (VANETs). For instance, drones move fast over the airspace limited by the airways; they communicate at the Line of Sight (LoS); and have Size, Weight and Power (SWaP) limitations [Boccadoro et al. 2021].

1.1. Problem Statement

Security and privacy are significant issues to be addressed in this novel and unique scenario. Since drones are in the airspace, various attack methods can be more harmful than grounded mobile networks [Tsao et al. 2022, Lin et al. 2018, Derhab et al. 2023]. Likewise, in other mobile networks, both the network infrastructure and the surrounding environment must have Protection Mechanisms (PMs) to ensure well-known security properties not just for drones but also for other elements of the environment [Gharibi et al. 2016, Derhab et al. 2023].

On the one hand, PMs have been investigated in other mobile paradigms [Boccadoro et al. 2021]. On the other hand, they have not been applied in IoD or even verified for the threats that can affect this environment. For instance, jamming attacks can hamper the IoD network communication, but differently as in VANETs. Thus, the design of PMs related specifically to IoD is in its initial steps. Therefore, some research questions arise, representing open challenges in the Computer Networks research field, precisely in IoD's security and privacy aspects.

- RQ1: *Can the existent protection mechanisms (from other mobile networks) provide the same protection level to IoD when compared to the mobile network environment of origin?*
- RQ2: *If* RQ1 *is false, is it possible to adapt an existing protection mechanism aiming to enhance the protection level provided to the IoD environment?*

1.2. Goals and Contributions

The main goal of this dissertation is **to study the design of PMs for the IoD paradigm, considering the particular characteristics of this environment**. To address this goal, we conduct a thorough study regarding the main concepts of IoD and its relationship with other networks, what are the attacks that threaten this environment, what are the existent PMs, and how these mechanisms mitigate the attacks [Svaigen 2023, Chapter 3]. From this study, we advance the state-of-the-art in the IoD security/privacy field on four different fronts:

(i) We propose a framework to guide the design of IoD-related PMs [Svaigen 2023, Chapter 3]. The design of all the subsequent PMs follows this framework.
(ii) Our central front of contributions relies on the design of Location Privacy Protection Mechanisms (LPPMs) for IoD [Svaigen 2023, Chapter 4].
(iii) We shed light on the impact of Jamming Attacks (JA) in the IoD, focusing on drone path planning and, therefore, the drone trajectory [Svaigen 2023, Chapter 5].
(iv) Last but not least, we introduce new approaches to Automatic Drone Detection (ADD) [Svaigen 2023, Chapter 6].

2. Attacks and Protection Mechanisms in IoD: Overview and Design Guidelines

The unique environment promoted by IoD leads us to analyze and classify UAV-related attacks from a new perspective. Therefore, we conducted an extensive survey about the attacks that can significantly affect the network due to its particular characteristics. From a comprehensive set of related studies, we surveyed seven major classes of attacks that can

be favored by IoD distinct characteristics, affecting the network deeply, mainly regarding the drone's mobility, availability, and privacy [Svaigen 2023, Section 3.1]. These attacks can be grouped according to their behavior, as passive or active. Furthermore, they are interlaced, so they can be combined as a pipeline, representing smart attacks. Most identified attacks also occur in other mobile networks, such as VANETs. Therefore, different PMs were designed in those networks. However, it does not mean they will perform properly in IoD, leading us to the research questions of this dissertation. Therefore, we first analyze what are the IoD environmental elements to protect. From that, we summarize six groups of PMs with potential use in IoD, examining what attacks they can mitigate and what elements they can potentially protect [Svaigen 2023, Section 3.2]. This analysis leads us to state trends and challenges in the security/privacy IoD field [Svaigen 2023, Section 3.3].

All these findings highlighted a major issue: unprecedented attacks can occur in IoD, or even well-known attacks can occur differently, posing several challenges for the design of IoD-related protection mechanisms. Therefore, we propose a framework to guide the design of protection mechanisms for IoD, representing the critical directions toward security and privacy. This contribution handles the current challenges in this area since it is still in its first steps. It is necessary to explore novel defense mechanisms and evaluate the performance of protection mechanisms stemming from other mobile networks [Svaigen 2023, Section 3.4]. Regarding this research front, we produced three technical surveys. The first concerns design guidelines for IoD-related PMs based on the proposed framework (Table 1, Ref. J3). The second survey discusses security/privacy aspects applied to the industry (Table 1, Ref. J4). The last focuses on analyzing the attacks in IoD through a privacy perspective (Table 1, Ref. U1).

3. Design of Location Privacy Protection Mechanisms for IoD

De-anonymization attacks (DAAs) represent a severe risk in IoD since they constitute a significant group of location privacy attacks, and this class of attacks is not properly investigated in the IoD research field. Through a comprehensive review of the literature, we note a need for studies studies regarding the design of Location Privacy Protection Mechanisms (LPPMs) in the IoD. Indeed, most proposed strategies are "ground-centered", taking advantage of terrestrial vehicular behavior to provide the required privacy level. Consequently, the airspace does not provide the necessary characteristics for the current LPPMs, justifying this investigation. We design three new LPPMs considering different scenarios. They are briefly discussed as follows.

3.1. t-MixDrones [Svaigen 2023, Section 4.2]

Based on the Mix-Zones (MZ) concept, t-MixDrones performs re-anonymizations of the drone pseudonyms, applying a bio-inspired approach to deploy MZs based on the traffic flow of drones dynamically. When a minimum number of drones are inside a specific MZ, these drones get new pseudonyms and can alter their airway altitude. This mechanism presents proper levels of location privacy in dense scenarios, although its application can cause an increase in power consumption due to the additional maneuvers.

3.2. MixRide [Svaigen 2023, Section 4.3]

This mechanism is also based on the MZ concept, promoting an air-to-ground collaboration between drones and public transportation. Drones take a ride in public buses in such

a way that the network assigns a vehicle for the drone to land and remain in silent mode. Hence, the grounded vehicle is a mobile MZ, where the drones change their pseudonyms while saving energy. MixRide provides better energy efficiency and lower communication overhead compared to t-MixDrones. However, MixRide can cause a delay in the drone's flight depending on the associated delay of public buses.

3.3. TDG [Svaigen 2023, Section 4.4]

TDG is an obfuscation LPPM that generates dummy queries based on the airways topology. When the drone needs to communicate with a location-based application, the mechanism produces k additional dummy queries with different locations, causing noise and obfuscating the actual drone location. TDG does not require a minimum number of drones to create the dummy queries, so the mechanism is suitable for sparse environments.

3.4. A Reinforcement Learning Approach for Dynamic Assignment of LPPMs [Svaigen 2023, Section 4.5]

Although these mechanisms present suitable levels of protection regarding location privacy, they were designed for specific scenarios. No mechanism can be considered a "silver bullet" for addressing optimal location privacy. Therefore, we model a Reinforcement Learning approach for the dynamic assignment of the proposed mechanisms, named IoDAPM. This approach covers the design of smart mechanisms, highlighted as one of the significant challenges in the IoD security/privacy research field. Through extensive simulations, we demonstrate the robustness of IoDAPM, ensuring that RL strategies can be applied to assign LPPMs in the IoD dynamically. IoDAPM outperformed the related IoD-based LPPMs, providing the highest level of QoS to the network, enhancing location privacy, energy efficiency, and flight delay, and also presenting a stable behavior regardless of the network conditions.

3.5. Case Study: Impact of Remote ID Rule in the Drone's Location Privacy [Svaigen 2023, Section 4.6]

Over the years, government authorities have been implementing measures to regulate the airspace. Recently, the Federal Aviation Administration (FAA) of the United States released the Remote ID rule for airspace monitoring. Any drone with a Remote ID must broadcast its sensitive information while operating over the airspace, which can threaten the drone's privacy. From an attacker's point of view, Remote ID allows a malicious entity to obtain enhanced knowledge about the drones since the attacker has a device with the Remote ID broadcast module. Therefore, we conduct a case study demonstrating that Remote ID threatens the drone's location privacy in the IoD environment. Also, we aim to analyze if existent protection mechanisms for IoD can be designed as an extension of the Remote ID to provide adequate location privacy.

Through the modeling of a Remote ID-centered location-based attack, the adaptation of existent LPPMs, and extensive simulations, we technically demonstrate that Remote ID is a serious threat to the drone's location privacy in the IoD, where more than 90% of the drone's trajectory can be tracked given an attacker with a Remote ID module. We also demonstrate that existing LPPMs can enhance the standard Remote ID protocol, mitigating the attack success and providing better location privacy for drones.

3.6. Some Comments About the Contributions

All the proposed mechanisms are compared to related traditional LPPMs of other networks. The conducted comparative evaluations highlighted that the proposed IoD-related LPPMs overcome the traditional ones in all simulated scenarios, providing a better security/privacy level to the IoD nodes considering a series of related metrics. Therefore, we can answer the two research questions of this dissertation considering LPPMs: The existent MZ and dummy-based LPPMs can not provide the same protection level to IoD environments. Fortunately, it is possible to adapt these existing LPPMs to enhance the protection level provided to a given IoD environment.

The design of LPPMs for IoD is the central front of the contributions of this dissertation, in which we produced eight technical papers. Initial discussions about the dynamicity of MZ mechanisms are published in an international conference (Table 1, Ref. C10). Three of them are derived from the design, analysis, and findings of t-MixDrones (Table 1, Refs. J2, C4, C7). The design of TDG and MixRide are covered in two papers published in top-tier international conferences (Table 1, Refs. C1 and C2, respectively). The findings of the conducted case study regarding Remote ID and the proposal of IoDAPM are also published in international conferences (Table 1, Refs. C6 and C7, respectively).

4. Design of Anti-Jamming Mechanisms for IoD

A Jamming Attack (JA) represents a severe risk in IoD because availability is a paramount requirement. There are some effective countermeasures against JA in terrestrial mobile networks. However, they are ineffective in IoD because they can not appropriately handle LoS-induced security issues. The relation between JA and the drone trajectory has been widely discussed in UAV-based networks [Svaigen 2023, Section 5.1], but those studies consider the airspace free to fly. In contrast, one of the most prominent characteristics of IoD is the presence of airways, allowing drones to fly over constrained airspace. Since the airways limit this flyable airspace, current solutions can not be applied directly to IoD.

Bearing these challenges in mind, we investigate the impact of JA on drone path planning and, therefore, its trajectory. From that, we design the IoD-JAPM [Svaigen 2023, Chapter 5], an airway-aware PM against JA on the IoD. The mechanism ranges from analyzing the airway's availability to reformulating the drone path planning. IoD-JAPM embraces: (i) a method to isolate a region affected by a JA in the IoD, considering the airway topology; (ii) a strategy to avoid a jamming signal in an affected region without violating the flight restrictions imposed by the airway; and (ii) and another strategy to mitigate the impact of the reformulated drone path planning when its final destination belongs to a region affected by the JA.

We conduct an experimental evaluation through simulations considering four different approaches presented in the literature [Svaigen 2023, Section 5.5]. We considered environments with varying airway topologies and various jammers performing attacks. IoD-JAPM overcomes the existing solutions in most scenarios, mitigating the effects of JA over the path planning, causing few reformulations or cancellations. Furthermore, IoD-JAPM causes a slight increase in the drone's original flight distance but provides better power consumption management. Therefore, we can answer the research questions of this dissertation by considering the design of anti-jamming mechanisms for IoD: considering IoD environments with well-defined airways, existing

anti-jamming mechanisms can not provide the same protection level for IoD. However, it is possible to adapt existing anti-jamming techniques to enhance the protection level in an IoD environment, as we demonstrated with IoD-JAPM.

Regarding this research front, we produced two technical papers. The first one is published in the SBRC Symposium, discussing our initial findings about the challenges posed by the relation between JA and the drone's trajectory (Table 1, Ref. C9). The second paper is published in a top-tier international journal, presenting our complete analysis and the IoD-JAPM design (Table 1, Ref. J1).

5. Design of Automatic Drone Detection Strategies for IoD

Automatic Drone Detection (ADD) can protect IoD nodes from unauthorized/unknown entities, being a silent and supportive mechanism for other PMs. Over the last few years, ADD has been improved by exploring innovative approaches integrated with traditional technologies and methods. However, there is room for improvement in this direction. For instance, although the current AI-based strategies address a suitable accuracy, the detection is dependable on known data. In other words, the approaches can properly detect authorized drones since they have a pool of samples from the expected categorization. Still, they fail to detect unknown entities and even distinguish different unauthorized UAVs.

This dissertation contributes to the ADD by introducing two new concepts: the study of using a drone's propeller acoustic signal as an input source; and the introduction of the dissimilarity concept to detect unknown UAV signals. These findings result in a smart strategy to detect drones through rhythmic-based features and a new detection mechanism, named DissIdent. The contributions correspond to initial findings regarding using rhythm properties and detecting through dissimilarity techniques. Hence, they make room for future research in this direction [Svaigen 2023, Chapter 6].

We conducted experimental evaluations comparing DissIdent with supervised-based and clustering approaches [Svaigen 2023, Section 6.5]. DissIdent overcame all the compared approaches in the detection and identification tasks, addressing accuracy rates of about 94% and 93%, respectively. The results also highlighted that the transformation from the feature to the dissimilarity space did not cause a loss of information for the training/classification model, promoting an enhancement in the detection of known signals and a significant improvement in the detection of unknown signals.

We produced two technical papers regarding this research front that were published in international conferences. The first one is related to the study of rhythm-based features (Table 1, Ref. C5). The second paper was published in a top-tier international journal, presenting the design and findings related to DissIdent (Table 1, Ref. C3).

6. Research Accomplishments

Over four years of doctoral studies, this research has generated fifteen publications. They are summarized in Table 1. Five papers were published in top-tier IEEE, ACM, and Elsevier periodic journals and magazines (four already published and one is under review). Furthermore, ten papers were published in IEEE, ACM international conferences, and a SBC national conference, including worldwide flagship conferences in the Computer Networks and Communications area, such as IEEE ICC and IEEE GLOBECOM.

Table 1. List of publications grouped by category and ordered by *Qualis CAPES* classification. Journal Impact Factor (IF) and Google Scholar H5-index (H5) and paper citations (GS) quality metrics are also presented.

Cat.	Ref.	Work	Qualis	IF	H5	GS
Journals	J1	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. (2023). Trajectory Matters: Impact of Jamming Attacks Over the Drone Path Planning on the Internet of Drones. **Ad Hoc Networks**, 146, 103179.	A1	4.8	59	7
	J2	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). BioMixD: A Bio-inspired and Traffic-aware Mix Zone Placement Strategy for Location Privacy on the Internet of Drones. **Computer Communications**. Vol. 195. pp. 111–123.	A2	5.1	82	14
	J3	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). Design Guidelines of the Internet of Drones Location Privacy Protocols. **IEEE Internet of Things Magazine**. vol. 5, no. 2, pp. 175-180, June	B1	3.5	28	12
	J4	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2023). Security in the Industrial Internet of Drones. **IEEE Internet of Things Magazine**. vol. 6, no. 3, pp. 110-116, September.	B1	3.5	28	3
Conferences	C1	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). A Topological Dummy-based Location Privacy Protection Mechanism for the Internet of Drones. In **IEEE ICC**, pages 3735–3740.	A1	-	76	9
	C2	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). MixRide: An Energy-Aware Location Privacy Protection Mechanism for the Internet of Drones. In **IEEE GLOBECOM**, pages 3527-3532.	A1	-	64	4
	C3	Svaigen, A.R., Boukerche, A., Ruiz, L.B., and Loureiro, A. A. F. (2023). DissIdent: A Dissimilarity-based Approach for Improving the Identification of Unknown UAVs, In **IEEE PIMRC**, pp. 1-6.	A1	-	30	1
	C4	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2021). MixDrones: A Mix Zones-based Location Privacy Protection Mechanism for the Internet of Drones. In **ACM MSWiM**, pages 181–188.	B1	-	19	25
	C5	Svaigen, A. R., Bine, L. M. S., Pappa, G. L., Ruiz, L. B., and Loureiro, A. A. F. (2021). Automatic Drone Identification Through Rhythm-based Features for the Internet of Drones. In **IEEE ICTAI**, pages 1417–1421.	B1	-	26	9
	C6	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). Is the Remote ID a Threat to the Drone's Location Privacy on the Internet of Drones? In **ACM MobiWac**, pages 81–88.	B1	-	19	8
	C7	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). Analyzing the UAVs Traffic Flow to Enhance the Drone's Anonymization on the Internet of Drones. In **ACM DIVANet**, pages 45–52.	B1	-	19	1
	C8	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2023). IoDAPM: A Reinforcement Learning Approach for Dynamic Assignment of Protection Mechanisms in IoD. In **ACM MSWiM**, pages 147–154.	B1	-	19	-
	C9	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. (2022). Um Mecanismo de Proteção Ciente de Vias Aéreas Contra Jamming Attacks para a Internet dos Drones. In **SBRC Symposium**, pages 405-418. SBC.	B2	-	8	1
	C10	Svaigen, A.R., Ramos, H.S., Ruiz, L.B. and Loureiro, A.A.. (2019). Dynamic Temporal Mix-Zone Placement Approach for Location-based Services Privacy. In **IEEE LATINCOM**. Pages 1-6.	B2	-	11	5
Unpub.	U1	Svaigen, A. R., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. F. Attacks in the Internet of Drones through a Privacy Perspective: Models, Trendings, and Challenges. **ACM Transactions on Internet of Things**. (First Round of Reviews)	-	-	-	-

Total papers: 15 / Average per year: 3.75 — Total Citations: 99 / Average per year: 24.75

This research has been conducted in collaboration with the PARADISE Research Lab (University of Ottawa, Canada), led by Dr. Azzedine Boukerche, a Distinguished University Professor and Senior Canada Research Chair Tier-1 at the University of Ottawa. Also, the Manna Research Group (State University of Maringá, Brazil) is a partner in this research. Being leaded by Dr. Linnyer B. Ruiz – President of the Brazilian Society of Microelectronics (SBMicro) and CNPq Research Productivity 1D Scholar) – Manna is the most extensive teaching teaching, research, extension, and innovation ecosystem in IoT and Robotics in the state of Paraná and one of the largest in Brazil.

7. Conclusion and Dissertation Impact

This dissertation tackled the challenge of the design of Protection Mechanisms for the IoD paradigm, considering the particular characteristics of this environment. This is one of the fundamental problems that must be solved towards the large-scale deployment of the IoD paradigm. Thus, we proposed a framework to guide the design of new PMs. From that, we designed IoD-related PMs to mitigate the effects of location privacy, jamming attacks, and the presence of unauthorized drones in the environment. In conclusion, all the proposed

mechanisms and strategies presented a unanimous answer to the research questions raised in this dissertation: the existing PMs (considering the investigated research fronts) can not provide the same protection level of security/privacy to IoD environments compared to traditional mobile networks. This answer justifies the need for the design of novel protection mechanisms so they can adapt to the existing ones or even new strategies.

The knowledge obtained from this research has been featured in several top-tier venues regarding scientific publications. The results of this dissertation have advanced the literature in several ways. The published surveys have been used as a guide to academia since they provided a technical and critical analysis of the current IoD security scenario. Also, the proposed framework has been leading the design of novel PMs for IoD. Similarly, the proposed PMs have been inspiring novel strategies to constantly enhance the security/privacy IoD levels. This dissertation also makes room for the observance of new challenges [Svaigen 2023, Chapter 7], such as the study of the remaining fronts of existent PMs, the study of utility preservation for anonymized data, the study of QoS provisioning, enhancement of ADD through dissimilarity-related techniques, design of collaborative and smart protection mechanisms for IoD, and the deployment and evaluation with testbed and real-world IoD infrastructures. Therefore, these challenges point towards new research directions in the IoD security/privacy field.

Acknowledgements

This work was partially supported by the CAPES, CNPq (grants 311685/2017-0, 421548/2022-3, 406193/2022-3, & 310620/2019-8), FAPESP (grants 15/24494-8 & 18/23064-8), NSERC CREATE TRANSIT, NSERC DIVA Strategic Research Network, Canada Research Chairs Program.

References

Bine, L. M., Boukerche, A., Ruiz, L. B., and Loureiro, A. A. (2022). Leveraging Urban Computing With the Internet of Drones. *IEEE Internet of Things Magazine*, 5(1):160–165.

Boccadoro, P., Striccoli, D., and Grieco, L. A. (2021). An Extensive Survey on the Internet of Drones. *Ad Hoc Networks*, 122:102600.

Derhab, A., Cheikhrouhou, O., Allouch, A., Koubaa, A., Qureshi, B., Ferrag, M. A., Maglaras, L., and Khan, F. A. (2023). Internet of Drones Security: Taxonomies, Open Issues, and Future Directions. *Vehicular Communications*, 39:100552.

Gharibi, M., Boutaba, R., and Waslander, S. L. (2016). Internet of Drones. *IEEE Access*, 4:1148–1162.

Lin, C., He, D., Kumar, N., Choo, K.-K. R., Vinel, A., and Huang, X. (2018). Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Communications Magazine*, 56(1):64–69.

Svaigen, A. R. (2023). *Design of Protection Mechanisms for the Internet of Drones*. Phd thesis, Federal University of Minas Gerais, Belo Horizonte, MG, Brazil.

Tsao, K.-Y., Girdler, T., and Vassilakis, V. G. (2022). A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-hoc Networks. *Ad Hoc Networks*, 133:102894.