On secure UAV collision avoidance

Thomas Ewert, Thomas Strang
Institute of Communications and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{thomas.ewert, thomas.strang}@dlr.de

***Abstract*—Over the last decade, connected vehicle research has extended from ground transportation into the airspace, with drones anticipated to play a central role in shaping the urban airspace ecosystem. Larger number of flights however also increase the risk of collisions proportionally. While some threats can be mitigated through Unmanned aeronautical vehicle Traffic Managment methods, such as conflict-free flight plans, an independent last line of defense is essential.**

DroneCast aims to address this need by providing a collaborative collision avoidance system based on broadcasted position reports of all drones. However, to prevent malicious actors from disrupting orderly traffic flow by injecting ghost targets that cause unnecessary avoidance maneuvers, robust cybersecurity measures are required.

This paper recaps strategies for securing DroneCast's broadcast messages given its resource-constrained environment. Beyond establishing robust cybersecurity measures, it further explores approaches for handling messages which can not be verified at the time and highlights their feasibility to deploy in real-world environments, laying the groundwork for future research.

***Index Terms*—UAV, Drone, Collision Avoidance, Broadcast Authentication, Digital Signatures, TESLA, MAC**

I. Introduction

In recent years, advances in technology have made drones an affordable and accessible mode of transport, primarily for goods but eventually also passengers in the near future. Use cases can be found in various industries, including defense or parcel delivery with companies like Amazon actively exploring ways to integrate drones into 'last-mile' delivery operations [1]. If these ambitious plans take shape, the number of drones over major cities could increase tremendously, and thus the risk of collision [2].

Current manned air travel relies primarily on Air Traffic Control (ATC), visual separation and the Traffic Collision Avoidance System to prevent mid-air collisions. While it is expected that Unmanned aeronautical vehicle traffic management will mainly avoid conflicts by pre-planning collision free trajectories and monitoring such throughout the system, the lack of redundancy would compromise the safety requirements common in any transportation domain. Existing systems from modern airliners could be repurposed for drones, but may introduce their inherited vulnerabilities [3], [4]. With the increasing ease with which potential attackers can acquire the necessary capabilities [5], using inherently insecure technologies for massive drone deployment is not advisable.

To minimize the risk of in-flight collisions, the German Aerospace Center (DLR) is developing a drone-to-drone communication and surveillance system within the DroneCast project, addressing the need for a last-line of defense. The technology is envisioned as a drone collision avoidance system in urban airspace, similar to existing systems used in conventional aviation [6]. It is based on periodical beacon messages broadcasted by every drone, consisting of position, speed and identifying information. Any other drone in reception range can then calculate a potential point of collision on their flight paths which in turn can be circumnavigated to avoid the collision from happening.

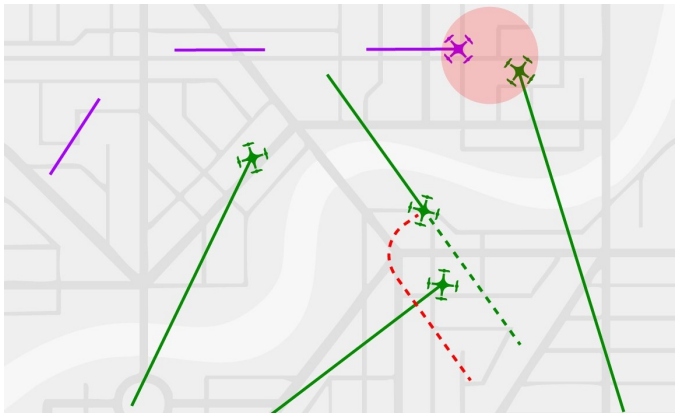

Fig. 1: The figure illustrates a DroneCast scenario where green drones transmit verifiable messages, enabling collision prevention through timely avoidance maneuvers (red track). In contrast, the purple drone's messages are not verifiable, representing a potential malicious actor. Additional strategies are therefore required to ensure safe interaction with such non-verifiable or adversarial participants (red circle).

Despite the fact that any of the cooperative anti-collision technologies in road, rail and air is meant to protect the safety of its users, there exist malicious forces trying to compromise those approaches for their very own benefit. For instance, one could try to keep drones from overflying their own properties by injecting position reports from artificial, non-existent ghost targets. Without sound cybersecurity measures, any drone would circumvent the area as no possibilities to distinguish such messages from authentic ones exist.

In the following, we introduce the DroneCast system shortly in Chapter II, and introduce the results of previous work on efficiently protecting its broadcast communication in Chapter

III. The paper then focuses on strategies to deal with messages, which are currently not verifiable, and highlights difficulties for real world implementations before giving an outlook on future work necessary in this domain.

II. Background

DroneCast is a communication system under development that provides collaborative detect-and-avoid functionality for collision prevention through broadcasts at regular intervals. It is designed as an independent system with the characteristics of urban mobility in mind and supports a minimum of 100 drones per surface square kilometer. Transmission is foreseen in a 5 MHz channel of the C-band between 5030 MHz and 5091 MHz, which has been allocated for drone communication in many countries. While the minimum reception range required for collision avoidance varies and depends on multiple factors, authors in [6] assume that a minimum system range of 1 km is sufficient for the urban environment.

To enable operation with a large density of drones, broadcast message duration is restricted to approximately 1 ms in length and a nominal rate of 1 Hz on average [7]. With providing situational awareness for all drones as the major goal, message content primarily focuses on speed and location information, but also contains operational information. Current drafts specify a 32-bit Cyclic Redundancy Check for error correction and reserve an additional 256 bits per message for security, resulting in a total broadcast size of 484 bits [6], [7].

Drones utilize the received position and speed vector data to determine the current proximity to the sender and anticipate any potential flight-path conflicts, allowing them to take corrective action if necessary. This, however, depends on successful reception and valid content of broadcast messages. To minimize message collisions, time is divided into frames which are further divided into slots. Each drone is assumed to transmit once per frame, but can only randomly select from a group of slots which is determined based on its own current position. Closely located drones therefore transmit on different slots which in turn reduces multiple-access interference [8]. While transmission through selected slots still results in broadcast messages at a 1 Hz rate on average, they are not evenly spaced over time. Previous work [9] identified authenticity and integrity as paramount to preventing insertion of malicious messages such as ghost targets. With the system's constraints in mind, the following chapter summarizes the results to ensure these properties.

III. Broadcast Security

In DroneCast, the security design is shaped by three central constraints: limited bandwidth, strict transmission intervals, and a large number of potential recipients. These factors restrict the applicability of otherwise common cryptographic primitives and necessitate tailored solutions. Prior work [9] has shown that symmetric Message Authentication Codes (MACs) provide efficient authenticity and integrity checks, but scale poorly in broadcast environments due to the need for shared keys between all communication partners [10]. Asymmetric digital signatures overcome this scalability issue, as each message can be verified using a publicly known key, but their larger size and higher computational cost make real-time authentication of frequent broadcasts challenging [11], [12]. A third option, Timed Efficient Stream Loss-tolerant Authentication (TESLA), leverages the efficiency of MACs while guaranteeing authenticity through delayed key disclosure, but it requires pre-computed key chains and introduces verification delays [13], [14].

To assess practical implications, we compared digital signatures and TESLA across storage, computation, transmission, and latency. Digital signatures require minimal storage—mainly keys and certificates—but impose high verification costs when processing thousands of broadcasts per second. Their signatures often exceed DroneCast's 256-bit limit, forcing multi-packet transmissions or excluding some algorithms. This makes them vulnerable to packet loss, since a missing fragment blocks verification until the next full signature. TESLA, by contrast, needs upfront storage of key chains (e.g., 113 KB for a two-hour flight at 1 Hz [9]) and careful expiration handling, but per-message computation remains lightweight. Verification delay equals the disclosure interval, typically one broadcast period, and resilience to loss is higher since later packets can reconstruct missing data.

Table I summarizes these trade-offs. Digital signatures integrate easily with PKI but strain DroneCast's bandwidth and real-time constraints. TESLA adds chain management complexity yet performs better under loss and remains compatible with future post-quantum schemes, where signature sizes will grow.

Property	Digital Signatures	TESLA
Latency	-	-
Computation	- -	+
Storage	+	-
Complexity	+	-
Packet Loss Resilience	-	++
Per-message Verification	-	+

TABLE I: Comparison of digital signatures and TESLA across key system properties.

The practical effect of these differences is further illustrated in Figure 2, which shows the average interval between two verifiable messages under different packet loss models. Digital signatures suffer sharp increases in verification delay whenever message fragments are lost, whereas TESLA maintains more consistent performance by leveraging key disclosure in subsequent transmissions. This resilience is particularly valuable in broadcast environments where overlapping transmissions and interference cannot be fully avoided.

Overall, we therefore recommend TESLA as the preferred solution for DroneCast authentication. In particular, its robustness to losses in non-deterministic broadcast channels and its suitability under stricter cryptographic regimes make it the most future-proof option, ensuring that broadcast integrity and authenticity can be maintained without fundamentally altering

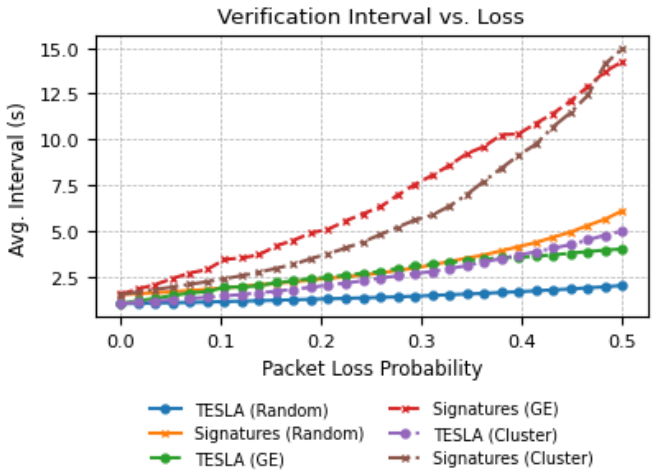

Fig. 2: Average interval between two verifiable messages using TESLA and digital signatures under different packet loss models. TESLA requires three packets to reach verifiability (1s), while signatures require four (1.5s). The Gilbert-Elliott (GE) model represents bursty losses by alternating between a low-loss and high-loss state, while the clustered model simulates loss bursts using random-length clusters.

system characteristics. Regardless of the chosen method, certain cryptographic information - such as a public key or the initial value of the TESLA hash chain, have to be available to all receiving drones. How to distribute such information efficiently is still to be defined.

IV. Handling of unverifiable messages

Even with robust broadcast authentication in place, message verification might not always be available immediately. This can be caused by system design (such as key-disclosure delays), packet losses or absence of required authentication information. The latter may result from delayed distribution of cryptographic material or from drones operating at airspace borders and receiving nearby traffic. Therefore, it should be considered how the system treats (*temporarily*) unverifiable messages so that safety is maintained while keeping an attackers possibilities to trigger needless avoidance maneuvers to a minimum. At the same time, the set of measures shall not be easily circumnavigated by any malicious actor. In the following, two complementary approaches - rule based filtering and lightweight machine learning detection - are introduced and the feasibility for real-world implementation discussed.

1) Rule-based Filtering: A simple approach is to apply domain-specific rules to filter incoming messages that violate expected protocol, kinematic or consistency checks. The latter exploits the fact, that ghost messages might include implausible or inconsistent state reports, which can be cross checked against physical limitations. Therefore, sudden large jumps in velocity or location, frequent jitter or unrealistic flight patterns such as hovering over the same location for extended period of times (”blocking” ghost example over private properties as indicated in the introduction) will raise red flags. If directional receiving antennas are available, signal direction or strength could be compared with the drone’s claimed position, with mismatches indicating spoofed sources. Such independent physical measurements have proven to be highly effective in spotting falsified location broadcasts [15]. Rule-based filtering have the advantage of causing only lightweight computational overhead due to basic arithmetic or logic checks and can therefore be implemented onboard within high dynamic broadcast environments.

If an incoming message fails a rule, it could be discarded immediately or flagged as suspicious pending further verification. Rather than a simple per package accept or drop decision, a more nuanced approach could be implemented using a trust score per sender. With each rule violation, points are added, causing the sender to be marked as malicious and disregarded if a certain threshold is exceeded. This way, sporadic anomalies or packet losses do not cause automatic distrust, but frequent anomalous broadcasts can be excluded from further processing. While being computational efficient, the main limitation of rule-based filtering is that an attacker might carefully craft messages within the defined limits and therefore evades detection.

2) Lightweight Machine Learning Detection: While rule-based filtering is an essential first layer, it may be insufficient to handle subtle attacks. Machine learning based models can be trained to detect such anomalies indicating spoofing or misbehavior. Due to the resource restricted environment of a drone, a lightweight online anomaly detector or small neural network needs to be chosen. This model could continuously predict either the next state of a drone or the probability that received messages can be trusted. Prior research in this domain has shown the efficacy of such techniques in, e.g., Long Short-Term Memory based spoofing detection for the Automatic Dependent Surveillance - Broadcast system without adding significant complexity to the system [16]. Other lightweight models such as one-class Support Vector Machines or small decision trees could perform binary classification in form of ”legitimate” vs ”malicious” decisions based on the available data, which could also include logical indicators. For example, if a drone claims to be nearby but the signal has just now been first received, the reported position is likely spoofed. The utilized models can be deployed in an online fashion, meaning the detector adapts to evolving operational patterns or environmental changes.

By analyzing a richer set of sequence patterns, machine learning-based detection benefits can identify potential subtle attacks mimicking, e.g., physical laws and subsequently fooling basic filtering. While already used in commercial drone detection systems, its application in safety-critical applications requires great caution. Model tuning is important to reduce false positives, while a precautionary approach to avoid ignoring real drones is beneficial. Further, models require representative training data and expertise to deploy and should be regularly validated. Any chosen approach must be

lightweight enough to run on the drone's onboard hardware, as offloading to a more powerful ground station is not envisioned within the DroneCast environment. However, only inference has to run locally, while model update and training could be conducted centrally for all drones after landing, using the collected message traces.

Training and evaluating such a model solely based on simulated data is not feasible, as only predefined flight patterns and attacker models would be represented. Since real-world data from DroneCast is still limited, the vast data needed for reliable training is unavailable. Future hybrid approaches could be promising, such as layering rules with ML to refine detection or using a majority-vote design where both must agree, though careful integration is needed to avoid blind spots. For now, we therefore focus on a purely rule-based strategy.

V. Conclusions

Within this paper, we have introduced DroneCast and summarized different approaches for broadcast authentication based on the system's limitations. While each approach has its merits, in environments where transmission loss is unavoidable, tolerance to loss becomes critical. TESLA emerged as the optimal solution, primarily due to its robust performance under such conditions. Regardless of the chosen method, any communication system may encounter situations where received messages cannot be verified immediately. Since collision avoidance is the primary goal, but unnecessary maneuvers should be minimized, a clear strategy for handling such cases is required. The paper presented two complementary approaches—rule-based filtering and machine learning—and compared their feasibility for real-world use. While machine learning may outperform simple rules, obtaining training data for a hypothetical system is difficult. We therefore provide an example of rules usable for a real-world implementation, aimed at handling messages that cannot yet be verified while reducing unnecessary processing and mitigating malicious attempts:

- Kinematic Plausibility: Discard messages that imply motion outside the limits for drones, i.e., speed and acceleration exceeding thresholds or sudden jumps
- Stationary Hover Detection: Penalize drones that report nearly identical positions in the air for extended periods of time
- Signal Plausibility: If available, compare received signal strength and direction with claimed broadcast position
- Temporal Consistency: Verify that broadcast rate (1 Hz) is mostly available with drones claiming nearby positions
- Identity Consistency: Ensure each ID maps to a single plausible trajectory, conflicting reports reduce trust.

A per-sender trust score should be maintained. Each violation adds penalty points, and drones exceeding a threshold are treated as malicious. Scores should decay over time to forgive transient errors, and once a message is successfully verified, the score should be reset to zero.

Future research could address the exact specification of rules, strategies for handling position uncertainties, and methods for collecting suitable datasets to enable machine learning-based approaches.

Acronyms

TESLA Timed Efficient Stream Loss-tolerant Authentication

References

[1] Tyler Greenawalt, "Amazon has launched our most advanced delivery drone yet—here's everything you need to know," https://www.aboutamazon.com/news/operations/mk30-drone-amazon-delivery-packages(accessed December 18, 2024), About Amazon, Tech. Rep., 12 2024.

[2] M. Doole, J. Ellerbroek, and J. Hoekstra, "Drone delivery: Urban airspace traffic density estimation," in *8th SESAR Innovation Days, 2018*, 2018, sIDs2018: 8th SESAR Innovation Days, SIDs2018 ; Conference date: 03-12-2018 Through 07-12-2018.

[3] G. Longo, M. Strohmeier, E. Russo, A. Merlo, and V. Lenders, "On a collision course: Unveiling wireless attacks to the aircraft traffic collision avoidance system (TCAS)," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 6131–6147. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/longo

[4] A. Costin, A. Francillon *et al.*, "Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices," *black hat USA*, vol. 1, pp. 1–12, 2012.

[5] T. Ewert and N. Mäurer, "Safety and security considerations on the airbus wake energy retrieval program "fello'fly"," 04 2023, pp. 1–12.

[6] L. M. Schalk and D. Becker, "Dronecast – analysis of requirements and discussion of first design decisions," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 2022, pp. 1–9.

[7] D. Becker and L. M. Schalk, "Dronecast - physical layer design and measurement-based simulation analysis for urban drone-to-drone communication scenarios," in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 2024, pp. 1–7.

[8] ——, "Dronecast - mac layer design and optimization," in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 2024.

[9] T. Ewert, T. Strang, and L. Jansen, "Stop seeing ghosts: UAV broadcast authentication," in *2025 IEEE/AIAA 44th Digital Avionics Systems Conference (DASC)*, Montreal, CA, 2025.

[10] C. Paar and J. Pelzl, *Understanding cryptography: A textbook for students and practitioners*. Springer Science & Business Media, 2009.

[11] N.-Q. Luc, Q.-T. Do, and M.-H. Le, "Implementation of boneh - lynn - shacham short digital signature scheme using weil bilinear pairing based on supersingular elliptic curves," *Ministry of Science and Technology Vietnam*, vol. 64, no. 4, pp. 03–09, December 2022, accessed: January 30, 2025. [Online]. Available: https://www.researchgate.net/publication/366530582

[12] T. Ewert, N. Mäurer, and T. Gräupl, "Improving usable ldacs data rate via certificate validity optimization," in *2022 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, 2022, pp. 1–9.

[13] N. Mäurer, M. Caamano Albuerne, D. Gerbeth, T. Gräupl, and C. Schmitt, "A secure broadcast service for ldacs with application to secure gbas," in *40th AIAA/IEEE Digital Avionics Systems Conference, DASC 2021*, Oktober 2021, pp. 1–10. [Online]. Available: https://elib.dlr.de/142726/

[14] S. Gewies and T. Strang, "Authentication of the medium frequency r-mode navigation message," in *4th European Workshop on Maritime Systems, Resilience and Security 2024 (MARESEC 24)*, ser. Proceedings of the MARESEC 2024. Zendoo, November 2024. [Online]. Available: https://elib.dlr.de/210067/

[15] M. Keizer, S. Sciancalepore, and G. Oligeri, "Ghostbuster: Detecting misbehaving remote id-enabled drones," 01 2024.

[16] J. Wang, Y. Zou, and J. Ding, "Ads-b spoofing attack detection method based on lstm," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 160, 2020. [Online]. Available: https://doi.org/10.1186/s13638-020-01756-8