Circumventing the Random Access Channel: New Concepts for Accessing a Command & Control Link for Unmanned Aircraft

Daniel M. Mielke*, *German Aerospace Center (DLR)*
*daniel.mielke@dlr.de

***Abstract*—Unmanned Aircraft (UA) are expected to considerably grow in importance for global aviation during the next years. Although a comparatively high level of autonomy is anticipated for UA, a reliable data link (Command and Control, C2-link) will be mandatory for their operation. The C2 link is used to exchange all information between UA and remote pilot, immediately required for operating the UA. This data is called non-payload data; examples are positioning information, telemetry data or flight trajectories, respectively. None of the currently available aeronautical communication standards can fulfill the requirements for such a multi-user, multi-point datalink in terms of reliability, flexibility, data integrity, robustness and latency. The C-Band Digital Aeronautical Communication System (CDACS) is a possible candidate for such a C2 link making use of modern communication techniques like Orthogonal Frequency Division Multiplex (OFDM) and SC-FDMA, [1], [2]. While CDACS development has so far focused on the general requirements and the waveform design, physical layer robustness also known as *PHY layer security*, e.g. against jamming/spoofing, has not yet been considered yet. One aspect of making CDACS more robust is hardening the login process of a user, in the case of CDACS a UA, into the network against such attacks. This login process is often realized using a Random Access Channel (RACH), that enables users not known to the base station access to the network. In this paper we discuss several concepts that try to avoid the traditional RACH, thus closing one potential vulnerability of the system.**

I. Introduction

MORE and more UAs are expected to enter the skies both in the controlled and uncontrolled airspace in the coming years. For example, the market for UAs in the European Union is expected to make up to $10\,\%$ of the European aviation market [3] during the next ten years. UAs are expected to perform some general aviation tasks without the need for any remote pilot input. Nevertheless a robust datalink between the UA and the remote pilot is mandatory to exchange all information immediately required to operate the UA, called Command and Control (C2) data. While the UA continuously reports status and telemetry information to the remote pilot, it receives flight trajectories and other control commands. The C-Band Digital Aeronautical Communication System (CDACS) is a modern approach to such a data link. First concepts have been presented in [2], however, the aspect of physical layer robustness has not been discussed yet. One of these aspects affects the access of a new, i.e. yet unregistered, user to a radio cell of the network. A common approach in contemporary wireless systems to this problem is a Random Access Channel (RACH). This paper will discuss alternatives to this approach as they can be applied to the CDACS system. The motivation to avoid the traditional RACH is to make the system more robust against attackers that try to avert the access of unregistered users to the network by blocking the RACH. Using RACH-jamming to attack wireless systems has been discussed in e.g. [4] and [5] for the mobile phone networks Global System for Mobile Communications (GSM) and Long Term Evolution (LTE), respectively.

The remainder of this paper is structured as follows: After providing some definitions in Section II we shortly describe the properties of a RACH in Section III. In Section IV we propose our alternative concepts on how to design a wireless system like CDACS without a RACH before we end the paper with a discussion in Section V.

II. Definitions

The following definitions will be used throughout this paper:

Random Access Channel

Digital communications systems are often described using different abstraction layers, e.g. the OSI layer model. Therefore it is often distinguished between a logical/protocol understanding of the RACH and the physical understanding of the RACH, often called Physical Random Access Channel (PRACH). Since this paper focuses on physical aspects of the RACH, we always address the PRACH when discussing the RACH if not denoted otherwise.

User

Generally speaking for wireless communication networks, a user is an entity that has a demand for resources and is served by the wireless network. A user is either a source (when acting as a transmitter) or a sink (when acting as a receiver) of data. In the case of CDACS, a user corresponds to an UA which is one endpoint of the wireless communication part of CDACS. While CDACS is designed for UAs, it is applicable to aviation in general and may support all aircraft with higher levels of automation, such as those capable of single pilot operations.

Base Station

A base station is the other end point of the wireless communication part of CDACS. It has the capability to serve multiple UAs.

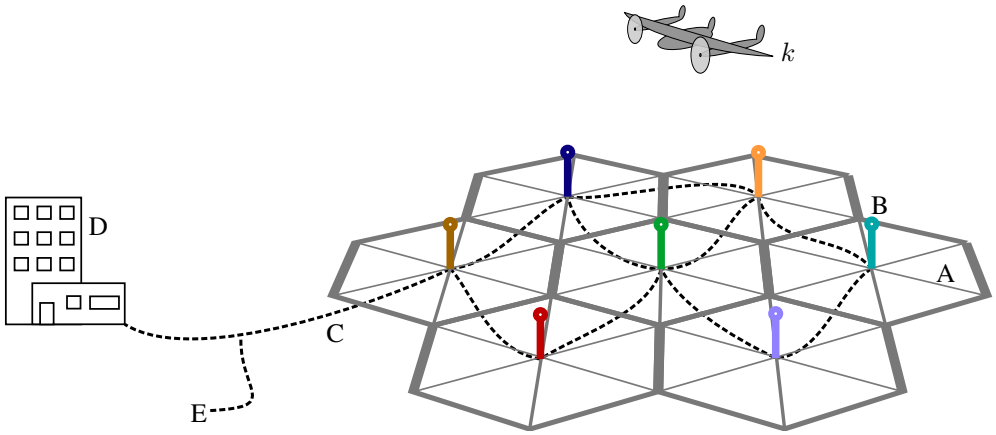

Fig. 1: Overview of CDACS: Radio cells like (A), represented by hexagons, are generated by base stations, e.g. (B). The radio cells might be split into several sectors (here: six sectors per radio cell) by applying beam forming. The base stations are connected by a backbone network sketched with dashed lines (C); remote pilots (D) are also connected to this backbone network. The backbone network is also accessible by a secure side channel (E). UAs, like k, try to establish a connection to the base stations and keep a connection alive during their entire flight. This implies establishing new connections when transitioning from one radio cell to another.

Radio Cell

A radio cell is the limited area in which bidirectional communication between a user and a specific base station, e.g. located in the center of the radio cell, is possible. It might be split into multiple sectors by applying antenna beam forming to the base station of the radio cell. Radio cells and base stations are sketched in Fig. 1.

Backbone Network

The backbone network is the network connecting all infrastructure required for a communication system like CDACS. This includes e.g. all base stations and gateways to other networks. The backbone network is assumed to be a secure network that only authorized entities have physically access to. It is responsible for routing all information to its dedicated receiver. The backbone network is sketched in Fig. 1.

Remote Pilot

The remote pilot is controlling and/or observing one or multiple UAs remotely, e.g. he or she is in charge of the flight trajectories the UA follows. The terminal the remote pilot is using to enter his or her commands or to receive status information is connected to the backbone network. The remote pilot is not necessarily closely located to the UA he is controlling.

Resource Allocation Authority

The Resource Allocation Authority (RAA) is responsible for allocating network resources to users in a network. Depending on the system's access technique, resources can be considered as

- a part of the spectrum (in case of Frequency Division Multiple Access (FDMA)),
- a time slot (in case of Time Division Multiple Access (TDMA)),
- a certain code sequence (in case of Code Division Multiple Access (CDMA)),
- a combination of all these access techniques.

The RAA is often realized as a scheduler, that is assigning resources to users under consideration of their specific demand.

Attacker

In this paper, we define an attacker as an entity that intentionally tries to disturb the regular processes inside a wireless communication system on the Physical-Layer (PHY) by emitting disturbing signals. This process is also known as jamming. We assume an attacker desires to continue the attack as long as possible, thus it tries to remain undetected or at least unlocated. A real world attacker is always limited in radiation power and bandwidth.

III. The Random Access Channel

A. Motivation

In multi-user networks, resources must be shared between all users. Multiple strategies have been developed over the years to fulfill this task. A common approach to this problem is a central instance (RAA), that is managing all resources in a network (or parts of a network like a radio cell) and assigns these resources to users. Modern wireless networks also consider individual resource demands of users to optimize the network capacity. However, the RAA must be aware of all users (and thus their demands) it is supposed to serve. While this is straightforward when a connection is already present

– the established data link can simply be used by the user to inform the RAA about its upcoming resource demand – this becomes more challenging in case a new user appears in the network. The new user cannot be considered by the RAA as long it is not informed about it, resulting in a classical chicken-and-egg problem.

A typical strategy of solving this problem used by many state-of-the-art wireless communication systems is a RACH.

Besides of making the network accessible to new users, the RACH can be also used to give the receiving base station a first idea of physically conditions of the wireless channel between the base station and the corresponding user, e.g. frequency and timing offsets. This information can be shared with the corresponding user once the connection is established so he can consider these information when composing its next message.

B. Technical Realization

Some network resources, e.g. certain time slots or frequency channels or CDMA-sequences, respectively, are reserved for the RACH and never assigned to a user in the network. A new user in the radio cell is assumed to know how to access the channel, i.e. he is aware of the position in time/frequency/code domain, e.g. by listening to the Base Station (BS)'s signal or by some side information. The user emits a Cell Entry Request (CER) message to inform the RAA via the BS about his demand for resources and starts waiting for a resource assignment for a certain amount of time T_{RA} afterwards. These steps are visualized in Fig. 2. When the RAA has successfully received the request, it informs the user about the resources assigned to him, e.g. using a control channel, and the regular communication can start. In case the new user does not receive a resource assignment within T_{RA}, it waits $T_{\mathrm{RC},1}$ before sending another CER to the RACH. Not receiving a resource assignment may happen multiple times in a row: Assuming the i-th retry, the waiting time is given by $T_{\mathrm{RC},i}$. In many systems, $T_{\mathrm{RC},i}$ is taken from a uniform distribution with exponentially growing bounds.

The motivation for an entropy-based waiting time is that the reason for a failed log-in might be the simultaneous CER transmission on the RACH of more than one user resulting in catastrophic interference. A fixed waiting time would lead to interfering CER messages for each retry until the RAA might be able to decode one user's CER, e.g. because of varying channel conditions.

By the time, a user tries to access the RACH, e.g. in case of TDMA a RACH-timeslot, he usually is not perfectly synchronized with the rest of the network. Thus, a RACH is designed to provide comparatively large guards to neighboring resources to reduce interference. In case of a TDMA based RACH, this would mean that the reserved width of the RACH slot is much wider than the length of the actual CER message. The new user tries to time his CER message such it arrives in the center of the RACH slot.

For the sake of completeness it should be noted that reserving certain resources to provide a RACH (including the required guards) decreases the overall bandwidth efficiency of a radio system. Nevertheless this effect is often considered as negligible and is not the main motivation for avoiding the RACH.

C. Scenarios where a RACH Is Used

Traditionally, a RACH is required for the following three scenarios:

1) Initial Network Login: The initial login is the first time the RF hardware is powered on and the user enters the system. This is realized by accessing a RACH and informing the RAA about the demand for resources in many systems. In fact, this might be the only realistic way to provide an initial login functionality for open systems like a cellphone network.

2) Cell Transition: In cellular networks, the process of transitioning from one radio cell (A) to another radio cell (B) is a common procedure when having moving users. It implies the logout from radio cell (A) and the login to radio cell (B). Assuming there is no advanced exchange of control information between the base stations of radio cell (A) and (B) (e.g. by using the backbone network), the login to radio cell (B) will be similar to the procedure of the initial network login - thus requiring a RACH.

3) Reconnect after Link Loss: Especially wireless communication suffers from disturbances of different origin like interference, bad Signal-to-Noise Ratio (SNR) or other channel effects that may make the channel unavailable for a certain amount of time. Particularly in aviation, this scenario is the most severe one since it describes a situation where the user (here: UA) is in a potentially unsafe state (i.e. UA is in the air and not grounded) and neither the event of a link loss nor the duration of such a loss is predictable.

A common approach for the detection of link losses is the exchange of keepalive (KA) messages between both communication partners on a regular base f_{KA} while the connection is established. A KA message does not necessarily need to contain any useful information as long as it is possible to determine its sender and perhaps the absolute time of transmission. Once no KA messages have been received for a time period of T_{TO}, the link is considered as down and the user is assumed to be logged out from its radio cell. Hence it is no longer considered by the RAA. To get the link reconnected, the user will access the RACH as he did during the initial cell login.

D. Possible Attacks

1) Jamming: Assuming a system with a RACH as described above, the only way a new user can inform the RAA about his demand for resources, independent of which of the three scenarios is assumed, is the CER. If the RAA is not able to process the CER or the user is not able to process the response message containing the resource assignment, a communication link cannot be established. This makes the login process, and thus the RACH, an extraordinary attractive target for an attacker, since he or she can focus his limited energy onto a small part of the overall system, nevertheless resulting in severe communication outages. The described attack is sketched for an TDMA-based RACH in Fig. 2c),

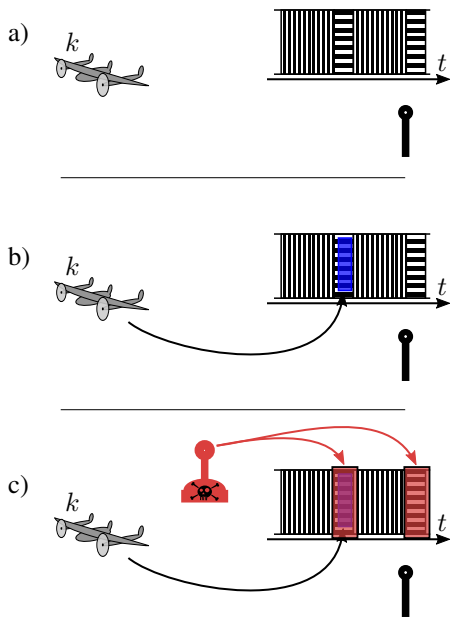

Fig. 2: Principle of a TDMA-based Random Access Channel: a) The base station is ready to receives data of registered users (vertical lines) and reserves time slots for the RACH (horizontal lines). b) k emits its CER message. Due to imperfect synchronization it does not perfectly match the time/frequency grid. However, the guards of the RACH prevent interference to adjacent resources. c) An attacker emits a pulsed jamming signal right into the RACH slot.

where the attacker is causing so much interference on the RACH, such that the base station is not able to successfully process the CER message of k.

For the attacker, the pulsed jamming approach has two advantages compared to an continuous emittance: On the one hand, RF hardware can usually emit higher peak powers than average powers – an effect that is often used in radar technology. On the other hand, the position of the attacker might be more difficult to determine, since no continuous signal is emitted.

2) Flooding: Another attack on the RACH can be performed aiming on higher protocol layers. For example, an attacker could emit a high number of faked CER messages resulting in a denial of service of the entities processing these request. Since this paper focuses on PHY layer aspects, this attack will not be discussed in more detail at this point.

IV. Strategies for Avoiding the RACH

In the following, we present alternative strategies for each of the scenarios defined in Section III-C.

A. Initial Network Login

In contrast to regular cellphone networks, a system as it is used for aviation can be understood as a closed system, where the location a device initially logs into the network is well defined since this location is always an airport. Thus we propose to perform the initial network login using a side channel (see Fig. 1 (E)) that is independent of the main system but still has access to the system's backbone network. We assume the side channel is also used to negotiate a set of shared secrets m_k between the UA and the backbone network once the connection is established. The initial network login must be completed before the UA leaves its parking position at the apron of an airport.

It shall be guaranteed that the side channel is inaccessible to unauthorized users. Taking nowadays airport architecture and security policies into account, this is an achievable condition for the following proposals for such a side channel:

1) Manual Login: An authority with direct access to the backbone network is informing the RAA of the radio cell covering the departure airport about the new user and its demand for resources. Since a remote pilot has access to the backbone network and is assumed as a trustworthy instance, he or she might inform the RAA about the new user in the network, including its Unique Identifier (UID), current position and so on.

2) Wired Connection: During the flight preparations of an UA, several physical connections exists between the airport infrastructure and the UA itself. Thus it is not too much of an effort to establish another physical connection providing a secure communication channel between the backbone network and the UA using a cable. However, an ultra-short range communication link like Radio-Frequency Identification (RFID) might be an alternative option in case the wired solution appears to be impractical.

3) AeroMACS: One possible candidate for a wireless side channel is Aeronautical Mobile Airport Communication System (AeroMACS), see e.g. [6], that is designed for airport-surface communications between grounded UA, airport authorities/management, all kind of airport vehicles, and airport buildings/devices. It provides data rates up to $9.2\,\mathrm{Mbit\,s^{-1}}$, encryption, and authentication features. Since it is only deployed in a limited and controlled area with restricted access, it is unlikely an attacker can apply any of the attacks discussed in Section III-D. However, even if the AeroMACS link was unavailable because of an attack (thus not able to support the initial login process), the UA is still in parking position on the apron, i.e. it is in a safe state.

B. Cell Transition

The transition from a radio cell A to a radio cell B is not necessarily a surprising event; ergo it can be prepared and planned if some side information is available.

The UA is equipped with several systems to determine its own position, e.g. Global Navigation Satellite System (GNSS) and Alternative Positioning, Navigation, and Time (APNT); besides it is aware of its most likely future flight trajectory. Both information is also available to the backbone network. Furthermore, we assume the UA carries an up-to-date database containing information on all base stations of the system, including antenna pattern, frequency and precise 3D position. Under these circumstances, both the backbone network and the UA can prepare the transition from one cell to another

unless no unforeseen events occur that require special event handling.

In preparation of a cell transition, the backbone network determines the next base station the UA will connect to based on its heading known from the side information. It informs the RAA of the specific base station about the resource demand of the arriving UA. It furthermore informs the UA about the base station that it is supposed to use next. Additionally, information on time and frequency offsets, determined by the current base station based on channel measurements and the Doppler shift, can be shared to improve the cell transition. Last but not least, higher protocol layer parameters like cryptographic keys can be exchanged between the new base station and the UA before the link to the old cell is disconnected.

This procedure is similar to *seamless roaming* that is part of certain wireless standards like LTE.

C. Reconnect after Loss of C2 Link

The link loss is detected the same way as described in Section III-C by using KA messages. However, we assume the KA message from the UA to the base station contains not only the UID of the sender, but also its current position (e.g. based on GNSS among other sources). Furthermore, the positioning information can be routed to the remote pilot since this is an important information for him anyway.

We present the following approaches on how a future aeronautical communication system could handle such an event:

1) Temporary RACH Approach: In case the base station detects the absence of KA messages of a user, it opens a traditional RACH for the cell the user just lost the connection to. The user continues to listen to the base station signal to detect when the RACH is opened and where it is located in time/frequency. Once it has detected the RACH slot it sends an CER message. When the connection between the base station and the UA is reestablished, the RACH is shut down again.

While this approach is straightforward, it is vulnerable to the attacks mentioned in Section III-D and a re-connection is likely to fail in case of an attack. This solution is not an option for a true RACH-free system and is only mentioned for the sake of completeness.

2) CDMA-Based Approaches: CDMA based systems benefit from spreading the information over a larger bandwidth than originally required (called spread spectrum) using a spreading sequence $\mathbf{c}_k$. This does not only enable the transmission of different data streams at the same time in the same frequency band, but also comes with a processing gain in the receiver. The latter property makes CDMA systems more robust against jamming attacks and is the main motivation why CDMA is often used in military applications [7].

In the following, we assume a $\mathbf{c}_k$ has been shared as part of set m_k during the initial network login. The reader may keep in mind m_k is assumed to be shared between the backbone network and UA k only, thus m_k and consequently $\mathbf{c}_k$ is not known to any possible attacker.

- The first approach is a simple application of CDMA to the temporary RACH approach described above: Once the base station recognized the link loss of UA k, it opens the RACH slot as before; however, it correlates all incoming data with the corresponding chip sequence $\mathbf{c}_k$. When the UA detects the link loss, it first tries to determine the RACH slot and then sends its CER message spread using $\mathbf{c}_k$. The application of CDMA will result in a processing gain depending on the chip sequence length making the system more robust against the attacks listed in Section III-D. Again, this approach is not totally RACH-free.
- The second CDMA-based approach introduced here works slightly different and does not require a RACH slot as the approaches presented so far. When a link loss of UA k is detected, the base station starts correlating the incoming data with $\mathbf{c}_k$ parallel to handling the incoming data of the other UA in the cell, i.e. a fallback channel is opened. At the same time, UA k starts repeatedly transmitting its CER message, again spread using $\mathbf{c}_k$. In contrast to the previous approach, no dedicated slot is used for transmitting the CER, resulting in a true RACH-free system. However, the transmission of the CER using the same resources (time and frequency) used by the other UA in the cell causes interference and may degrade the performance of their communication links. To mitigate this, the RAA of the base station can force the UA in the cell to use the most robust coding and modulation scheme available when opening the fallback channel. Additionally, traditional Successive Interference Calculation (SIC) approaches may be applied, e.g. the spread CER message can be subtracted from the incoming signal after it got successfully decoded.

3) Side Information Based Approach: This approach makes use of as much side information available to the backbone network and the UA as possible, including:

- Up-to-date information on all base stations (positions, frequencies, antenna pattern)
- Real-time information on the current position of the UA
- Continuously updated information on the 4D flight trajectories of the UA

Besides, we assume the UA to be equipped with a reliable high precision time source, e.g. a GPS-disciplined oscillator. This enables the capability to remain in a synchronized state with respect to the backbone network even if the communication link is unavailable for a certain amount of time.

The actual procedure of the backbone network in case a link loss to UA k is detected is as follows:

- The base station detects the link loss. It informs all other air vehicles in the area about the connection loss to k.
- Although the link is offline, the base station's RAA still reserves resources for UA k - just enough to receive its CER message. The resource assignment is broadcasted in the logical control channels so that the disconnected UA k is able to transmit its CER message correctly once it successfully received and processed a frame of the base station. This resource assignment is assumed to be inaccessible by an attacker, e.g. due to encryption

using a shared key from m_k. We call this blind resource assignment the *search mode*.
- The backbone network continuously estimates the position of the UA based on the side information and adapts the respective search area, i.e. the search mode is continuously expanded to all radio cells the UA could have possibly entered since the link loss was detected. Obviously, the search area consists of an increasing number of radio cells the longer the UA is not connected to any other base station. The backbone network might consider alternative sources to estimate the missing UA's position, e.g. by taking received Automatic Dependent Surveillance - Broadcast (ADS-B) messages into account, to keep the search area only as large as necessary.
- Once the UA was able to successfully login into a radio cell, either the one it lost its link to or another one, the backbone network informs all base stations to terminate the search mode for UA k.
- If the UA cannot be found for a longer period of time, an emergency case (e.g. fatal crash) is assumed. We suggest a manual termination of the search mode for UA k by an authority with access to the back bone network once the situation is clarified.

Correspondingly, the procedure of UA k in case of a link loss is as follows:

- In case a traditional aircraft transponder is present, it shall be switched to mode 7600 (Radio Failure)[1].
- The UA follows the latest flight trajectory successfully received from the remote pilot.
- Based on its position and flight trajectory, the UA selects one or more base stations that appear reasonable to connect to. The base stations' positions and channel frequencies are read from the onboard database.
- The onboard radio is configured to receive frames from the selected base station(s).
- A CER message is transmitted once a base station's frame was received, and the control channel was decoded and contained a resource assignment for UA k.
- The UA repeats this procedure until it received a response to its CER message and a link gets re-established. Then it switches its aircraft transponder back to the default mode if present.

V. Discussion

Investigating alternatives for the traditional RACH under the premise of the three scenarios identified in Section III-C showed that the scenario of the unexpected link loss appears to be the most critical one. In the following we want to discuss our proposed strategies for this event.

Since a *temporary RACH* suffers from similar vulnerabilities as a traditional RACH, it does not provide a huge security gain. Thus we do not consider this as an effective approach.

Securing the temporary RACH using CDMA as suggested in our next approach will increase the robustness thanks to the processing gain in the receiver. At the same time, it reduces the risk of catastrophic interference when two UA k and l are accessing the RACH simultaneously since there is a chance that the involved UA use different sequences $\mathbf{c}_k \neq \mathbf{c}_l$. Although the number of CDMA sequences available (corresponds to the key space in cryptography) is limited, an attacker would still need to use the exact same CDMA sequence to compensate the processing gain completely which becomes less likely the more sequences are available. Nevertheless, this approach is still vulnerable to jamming [7], especially since the spreading in frequency domain and consequently the processing gain will be limited to the channel bandwidth.

The second CDMA based approach is expected to be more robust against jamming since the CER is spread over a larger bandwidth; thus the spreading factor is higher. However, this approach adds interference to the communication channels of other users close to the CER-emitting UA. The suggested SIC will cause processing delays that may not be acceptable.

The last approach appears to be the most interesting one since the concept of transmitting CER messages in a way that is predictable to an attacker is completely dropped. Thus the transmission of CER messages cannot be attacked in a precise way and the attacker cannot benefit from focusing his or her available energy just onto a small portion of the system.

VI. Conclusion and Outlook

In this paper we have identified scenarios in which a traditional RACH is used and how the existence of a RACH might help an attacker to efficiently disturb communication in a wireless system. We have then investigated possible alternatives for these scenarios, taking the special properties of a closed system like CDACS into account.

We understand this as one first step towards making CDACS more robust against attacks on the PHY.

[1]The launch of unmanned aviation might have effects on the ICAO transponder codes and a new code representing *C2 link connection lost* might be implemented. In this case, this new code should be used.

References

[1] D. M. Mielke, "C-band digital aeronautical communication for unmanned aircraft systems," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, Sep. 2017, pp. 1–7.

[2] D. M. Mielke, "Frame structure of the c-band digital aeronautical communications system," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, April 2018, pp. 2C4–1–2C4–12.

[3] "Ip/14/384: European commission calls for tough standards to regulate civil drones," 2014. [Online]. Available: http://europa.eu/rapid/press-release_IP-14-384_en.htm

[4] M. R. Ståhlberg, "Radio jamming attacks against two popular mobile networks," 2000.

[5] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, April 2016.

[6] B. Kamali, *AeroMACS: An IEEE 802.16 Standard-Based Technology for the Next Generation of Air Transportation Systems*, 1st ed. Standards Information Network IEEE Press, 2018.

[7] R. A. Poisel, *Introduction to Communication Electronic Warfare Systems*, 2nd ed. Norwood, MA, USA: Artech House, Inc., 2008.