Securing the Skies: AKAASH Integration for Resilient CPDLC Communication

Xingkang Xue*

Department of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

Abstract

As Controller-Pilot Data Link Communication (CPDLC) becomes the standard in aviation communication, replacing traditional voice-based Air Traffic Control (ATC) systems, the industry benefits from increased resilience and bandwidth efficiency. However, this transition also introduces heightened cybersecurity concerns, with potential cyber-attacks targeting CPDLC infrastructure posing significant risks. In response, AKAASH emerges as a lightweight solution providing robust authentication, key establishment, and handover mechanisms. This mini review examines the importance of CPDLC, the cybersecurity challenges it presents, and the role of AKAASH in enhancing CPDLC communication security.

Keywords: Controller Pilot Data Link Communication (CPDLC) • Aviation communication • Voice-based air traffic control

Introduction

As Controller-Pilot Data Link Communication (CPDLC) becomes the global standard, replacing traditional voice-based Air Traffic Control (ATC) systems, the aviation industry gains resilience and bandwidth efficiency. However, the increasing reliance on CPDLC also brings about heightened cybersecurity concerns. Cyber-attacks targeting CPDLC infrastructure pose severe risks to individuals, stakeholders, and the aviation industry at large. In response to these threats, AKAASH emerges as a lightweight solution offering robust authentication, key establishment, and handover mechanisms. This mini review explores the significance of CPDLC, the cybersecurity challenges it faces, and the role of AKAASH in fortifying CPDLC communication [1].

Literature Review

The transition from voice-based ATC systems to CPDLC represents a significant advancement in aviation communication technology. CPDLC enables more efficient and reliable communication between pilots and controllers, enhancing operational efficiency and safety in airspace management. By leveraging data link communication, CPDLC reduces the reliance on voice communication, mitigating the risks associated with human error and language barriers [2].

Discussion

Despite its benefits, CPDLC is susceptible to cyber-attacks that can compromise the integrity, confidentiality, and availability of communication channels. Cyber-threats targeting CPDLC infrastructure include unauthorized access, data manipulation, and denial-of-service attacks. Such attacks not only endanger the safety of flight operations but also disrupt air traffic management systems, leading to significant economic and reputational damage. AKAASH offers a comprehensive solution to bolster the cybersecurity of CPDLC communication. By providing lightweight authentication, key establishment, and handover mechanisms, AKAASH enhances the security posture of CPDLC networks. The integration of AKAASH into the existing CPDLC framework enables seamless adoption without compromising operational efficiency. AKAASH's ability to adapt to diverse CPDLC environments ensures compatibility and interoperability across different aviation systems [3-6].

Conclusion

As CPDLC continues to proliferate globally, ensuring the security and integrity of communication channels is paramount. Cyber-attacks targeting CPDLC infrastructure pose significant risks to aviation safety, necessitating robust cybersecurity measures. AKAASH emerges as a promising solution to fortify CPDLC communication, offering lightweight yet effective authentication, key establishment, and handover mechanisms. By integrating AKAASH into existing CPDLC frameworks, the aviation industry can enhance resilience against cyber threats while maintaining operational efficiency and safety standards. Continued research and collaboration are essential to stay ahead of evolving cybersecurity challenges in CPDLC communication.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Gurtov, Andrei, Tatiana Polishchuk and Max Wernberg. "Controller–pilot data link communication security." *Sens* 18 (2018): 1636.

2. Glaser-Opitz, Henrich and Leonard Glaser-Opitz. "Evaluation of CPDLC and voice communication during approach phase." *IEEE* (2015): 2B3-1.

3. Brown, John Allin. "Human Factors Issues in CPDLC." *Routledge dict* (2017).

4. Rossi, Magali Andreia, Paolo Lollini, Andrea Bondavalli and Italo Romani de Oliveira, et al. "A safety assessment on the use of CPDLC in UAS communication system." *IEEE* (2014) 6B1-1.

5. Herrero Montolio, Joel. "CPDLC digital communication implementation between an ATC and RPAS." (2015).

6.   Shingledecker, Clark, Stephen Giles, E. R. Darby and Joseph Pino, et al. "Projecting the effect of CPDLC on NAS capacity." 1 (2005): 8.