VII International Conference on Mathematics and its Applications in Science and Engineering
(ICMASE 2026)

ICMASE 2026

MATHEMATICAL ANALYSIS OF NONCE GENERATION IN MAVLINK-BASED UAV COMMUNICATION SYSTEMS

Samuel Ela Nsogo Nsa[1], Raquel Cervigón Abad[2], Araceli Queiruga Dios[3,*]

[1]*PhD Programme Computer Engineering, Universidad de Salamanca*
[2]*Polytechnic School Cuenca, Universidad de Castilla la Mancha*
[3]*Institute of Fundamental Physics and Mathematics, Universidad de Salamanca*

ABSTRACT

Unmanned Aerial Vehicles (UAVs) rely on communication links to exchange telemetry, navigation data, and control commands between onboard flight controllers and ground control stations. In many UAV platforms this communication is implemented using the MAVLink protocol, a lightweight binary protocol designed for resource-constrained embedded systems and low-bandwidth links [1]. While MAVLink 2 introduces a message signing mechanism that provides authentication and integrity, it does not protect the confidentiality of transmitted data. Consequently, telemetry and control commands remain observable to adversaries capable of monitoring the communication channel.

To address this limitation, several works have proposed integrating cryptographic mechanisms into MAVLink-based communication stacks. In particular, lightweight authenticated encryption schemes are well suited to embedded UAV systems due to their low computational and energy requirements. Among these algorithms, Ascon-AEAD128 has recently been standardized by the National Institute of Standards and Technology (NIST) as the primary lightweight authenticated encryption algorithm for constrained devices [2]. The algorithm was specifically designed for environments such as embedded systems and Internet-of-Things platforms, where computational resources and power consumption are limited [3].

However, the security guarantees of nonce-based authenticated encryption schemes rely critically on the *nonce-respecting* assumption: the same nonce must never be reused with the same secret key. While this requirement is simple at the algorithmic level, it becomes significantly more subtle when the encryption primitive is integrated into an existing communication protocol. In particular, MAVLink packets include a sequence number field encoded on eight bits, which evolves according to modular arithmetic and necessarily wraps around after 256 transmitted packets. From a mathematical perspective, this behavior corresponds to the dynamics of a finite cyclic group and introduces deterministic periodicity in protocol state variables.

In this work we develop a mathematical framework for analyzing nonce generation in MAVLink-based communication systems using Ascon-AEAD128. Packet transmissions are modeled as a discrete state process in which the system state evolves with each transmitted packet. Nonce generation is represented as a deterministic function defined on the protocol state space, allowing the security requirement of nonce uniqueness to be formulated as an injectivity condition along the operational trajectory of the system.

Using this model, we analyze several natural nonce constructions derived from MAVLink packet fields. In particular, we show that constructions based directly on protocol sequence numbers lead to deterministic nonce collisions due to modular wraparound. Similar failures occur when the nonce is constructed by concatenating several protocol header fields, since some of these identifiers typically remain constant during a communication session. We also analyze random nonce generation and show that while deterministic collisions disappear, the probability of probabilistic collisions follows the classical birthday bound from applied cryptography [4].

[*]*Corresponding Author's E-mail: abc@hbv.edu.tr*

Finally, we study a session–counter construction in which the nonce is generated by combining a session identifier with a monotonically increasing counter. We prove that, under mild operational assumptions, this construction guarantees nonce uniqueness while remaining compatible with the constraints of UAV telemetry systems. The analysis highlights that the secure integration of authenticated encryption in communication protocols depends not only on the cryptographic primitive but also on the mathematical properties of the protocol state variables used to generate nonces.

The proposed framework provides a systematic approach for analyzing nonce generation in lightweight cryptographic systems and may serve as a basis for designing secure MAVLink-based UAV communication architectures.

***K*eywords** MAVLink protocol · Nonce generation · Lightweight cryptography

References

[1] MAVLink Development Team: MAVLink Protocol Overview. https://mavlink.io/en/about/overview.html (2024)

[2] Sönmez Turan, M., McKay, K., Chang, D., Kang, J., Kelsey, J., Peralta, R.: Ascon-Based Lightweight Cryptography Standards for Constrained Devices. NIST Special Publication 800-232 (2025)

[3] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology 34(3), 33 (2021)

[4] Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press (1996)