

A method for protecting UAV command link transmission using pseudo-random frequency hopping based on a parametric oscillator

Semen Zhyla^{1,†}, Kyrylo Muzychenko^{1,*,†} and Victor Yerokhin^{2,†}

¹State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zaliznyak Str., 3, Kyiv, 03142, Ukraine

²Military Institute of Telecommunications and Informatization named after the Heroes of Kruty, Ostrozkykh Kniaziv Str., 45/1, Kyiv, 01011, Ukraine

Abstract

This article proposes a novel method for protecting UAV command link transmissions, combining jamming resistance and spoofing resistance through pseudo-random frequency hopping (PRFH) implemented by a Mathieu–Duffing parametric oscillator. The mathematical model of the chaotic regime is presented in detail, including the conditions for parametric resonance onset, computation of the Lyapunov exponent, and phase portrait analysis. A complete block diagram of the transceiver path is developed with a thorough description of all functional units and inter-block connections. An original algorithm for coupling the chaotic frequency sequence with the command signal in Fast Frequency Hopping (FFH) mode is proposed. A comparative cryptographic analysis against classical PRFH systems is carried out and the advantages of the proposed approach are justified.

Keywords

unmanned aerial vehicle, jamming resistance, spoofing resistance, pseudo-random frequency hopping, parametric oscillator, Mathieu–Duffing chaos, Lyapunov exponent, phase portrait, command channel, synchronization

1. Introduction

Modern UAV radio command links operate in an increasingly hostile electromagnetic environment characterised by unintentional broadband interference, co-channel congestion in shared spectrum, and deliberately engineered electronic attacks. Three threat categories are of particular concern for the command channel. First, *electronic jamming*: a high-power broadband or spot-frequency signal is radiated toward the UAV to prevent the receiver from detecting legitimate commands. Second, *interception and decryption*: a passive adversary records the transmitted waveform and attempts to recover the command content, possibly with the aid of machine-learning classifiers. Third, *command spoofing*: the adversary injects syntactically valid but unauthorised command packets to seize control of the vehicle or cause mission failure.

Disruption of the command channel has immediate, irreversible consequences compared with loss of telemetry or video payload. A UAV that ceases to receive authenticated commands within a few hundred milliseconds will either execute a fail-safe return-to-home manoeuvre or become a hazard. This asymmetry justifies dedicating the highest level of protection to the Command and Control (C2) channel.

Frequency Hopping Spread Spectrum (FHSS) has been the canonical defence against both jamming and interception since the early work of Dixon [1] and Sklar [2]. In an FHSS system the carrier is shifted pseudo-randomly among N_{ch} pre-agreed channels at a rate that exceeds the adversary's ability to track and jam individual hops. The jamming resistance gain grows logarithmically with the number

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

[†]These authors contributed equally.

✉ Simeon.zhyla@gmail.com (S. Zhyla); kirilmuzychenko@gmail.com (K. Muzychenko); stddssss@gmail.com (V. F. Yerokhin)

ORCID 0000-0003-2989-8988 (S. Zhyla); 0009-0004-0738-6273 (K. Muzychenko); 0000-0001-7194-8577 (V. F. Yerokhin)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

of channels: a jammer must spread its power across the entire band, reducing its effectiveness per channel by a factor of N_{ch} .

Classical FHSS implementations rely on linear feedback shift registers (LFSRs), Gold codes, or maximum-length (m-) sequences to generate the hopping pattern. These generators are deterministic and algebraically structured, which exposes them to the Berlekamp–Massey attack [3]: an adversary who observes as few as $2n$ consecutive symbols of a degree- n m-sequence can reconstruct the entire internal state and predict all future hops. Gold codes fare somewhat better but remain vulnerable after intercepting 200–500 symbols [4]. Once the hopping sequence is known, jamming degenerates to a trivial spot-frequency problem and spoofing becomes feasible.

The central contribution of this work is the replacement of the algebraic LFSR with a *nonlinear parametric oscillator* operating in deterministic chaos. The Mathieu–Duffing oscillator, obtained by adding cubic stiffness and dissipation to the classical Mathieu equation, exhibits sensitive dependence on initial conditions quantified by a positive Lyapunov exponent $\lambda_{\text{max}} > 0$. Because the sequence $\{f_k\}$ is generated by a continuous-time chaotic flow sampled at discrete instants, its future values are provably unpredictable to any observer who does not know the initial state with machine-precision accuracy. Yet the sequence is perfectly reproducible at the receiver, which holds an exact digital replica of the oscillator initialised from the same secret state — making synchronisation possible while preserving cryptographic strength.

The remainder of this article is structured as follows. Section 2 surveys related work on FHSS security and chaotic communications. Section 3 states the article’s objectives. Section 4 constitutes the main technical contribution: mathematical analysis of the chaotic regime (Section 4.2), block diagram of the transceiver (Section 4.3), coupling and synchronisation algorithms (Sections 4.4–4.6), and a comparative cryptographic assessment (Section 4.7). Section 5 presents conclusions and directions for future work.

2. Review of related work

The security of FHSS radio links for UAV command and control has attracted growing attention as unmanned platforms proliferate in both civil and military applications. General FHSS principles and spread-spectrum theory are covered in the foundational monographs of Dixon [1], Sklar [2], and Proakis [5]. The specific challenges posed by UAV communication links — including beyond-visual-line-of-sight (BVLOS) scenarios, highly dynamic channel conditions, and the need to share spectrum with commercial aviation — are examined in [6, 7, 8].

On the cryptanalytic side, Golomb [3] established that m-sequences of degree n can be recovered from $2n$ intercept bits, while Meier and Staffelbach [4] showed that fast correlation attacks on certain LFSRs require only modest computational effort. A comprehensive survey of modern correlation attacks is given in [9].

The use of chaotic signals for secure communications was pioneered by Pecora and Carroll [10], who demonstrated that two identical chaotic circuits can synchronise when one drives the other. Cuomo and Oppenheim [11] showed how a chaotic masking waveform can conceal an information-bearing signal, and Kolumban *et al.* [12] formalised the role of synchronisation in digital chaotic communications. Subsequent work by Sobiski and Thorp [13] and Eisencraft *et al.* [14] extended these ideas to bandlimited channels. The application of chaotic oscillators specifically to PRFH — as opposed to direct-sequence spread spectrum — was explored in [13, 14], though those works focused on spectral spreading rather than on driving a discrete frequency synthesiser. The rigorous mathematical treatment of parametric chaos appears in Nayfeh and Mook [15] and Moon [16]. To the best of the authors’ knowledge, a complete synthesis of a UAV command-link PRFH system based on a parametric oscillator, including full transceiver architecture and synchronisation algorithms, has not previously appeared in the open literature.

3. Article objective

The objective of this article is to develop and justify a method for protecting UAV command link transmissions using PRFH based on a Mathieu–Duffing parametric oscillator. Specifically, the article aims to:

- provide a rigorous mathematical justification of the oscillator’s chaotic regime, including analysis of the phase portrait, Poincaré section, and Lyapunov exponent;
- develop a complete block diagram of the transceiver path with detailed specifications of all functional units;
- describe the algorithms for coupling the chaotic frequency sequence with the command signal, for acquisition and tracking synchronisation, and for multi-level spoofing rejection.

4. Main content

4.1. Justification for selecting the command channel

The radio link of a modern UAV encompasses three functional channels: the Command and Control (C2) channel, the telemetry channel, and the payload (video) channel. Each has distinct requirements that call for a tailored protection strategy.

The C2 channel transmits relatively short packets — typically 128–256 bytes including headers and authentication fields — at low symbol rates of 1–10 kbit/s, with a latency budget of no more than 100–200 ms. The low instantaneous data rate means that even a very high hopping speed does not significantly reduce throughput. A single hop need carry only a fraction of one symbol; thus the channel supports the *Fast Frequency Hopping* (FFH) regime, in which the carrier hops $N_{\text{FFH}} \geq 4$ times per transmitted symbol. This redundancy enables majority-vote decoding across hops, providing additional protection against frequency-selective fading and narrowband spot jammers.

The telemetry channel (10–100 kbit/s) is less latency-critical and can be protected by an analogous method operating at a lower hopping rate. The payload channel (video, typically several Mbit/s) requires a fundamentally different approach and is outside the scope of this article.

4.2. Mathematical model of the parametric oscillator

4.2.1. General equation of the parametric oscillator

A parametric oscillator is an oscillatory system in which one or more parameters vary explicitly with time. The canonical example is the *Mathieu equation*:

$$\ddot{x} + [\omega_0^2 + \varepsilon \cos(\Omega t)]x = 0, \quad (1)$$

where x is the generalised coordinate, ω_0^2 is the natural frequency of the unperturbed system, ε is the depth of parametric modulation, and Ω is the frequency of parameter variation. Equation (1) is linear and therefore produces only bounded stable oscillations or exponentially growing instability — no chaos. To generate chaos a nonlinear restoring force must be introduced.

4.2.2. The nonlinear Mathieu–Duffing oscillator

Adding cubic stiffness (the Duffing term) and viscous damping to (1) yields the *Mathieu–Duffing* oscillator:

$$\ddot{x} + 2\gamma\dot{x} + \delta x + \varepsilon \cos(\Omega t)x + \alpha x^3 = \xi(t), \quad (2)$$

where γ is the damping coefficient, α is the nonlinearity (cubic stiffness) coefficient, and $\xi(t)$ is weak zero-mean stationary white noise with intensity σ^2 , satisfying $\sigma \ll \varepsilon\omega_0$. The noise term ensures that the trajectory remains ergodic within the attractor and prevents long-term phase locking that could

otherwise freeze the orbit at a periodic sub-attractor. Without this small stochastic perturbation, finite-precision digital arithmetic occasionally drives the trajectory into a periodic window of the bifurcation diagram, making the output predictable for short intervals; the noise eliminates this hazard without qualitatively altering the chaotic dynamics.

For numerical integration by the 4th-order Runge–Kutta method, equation (2) is rewritten as a first-order system:

$$\dot{x}_1 = x_2, \quad (3)$$

$$\dot{x}_2 = -2\gamma x_2 - \omega_0^2 x_1 - \varepsilon \cos(\Omega t) x_1 - \alpha x_1^3 + \xi(t). \quad (4)$$

This system is autonomous in the extended phase space $x_1 x_2 \varphi$, where $\varphi = \Omega t \pmod{2\pi}$ is the phase of the external excitation. The extended phase space is a three-dimensional manifold $\mathbb{R}^2 \times S^1$ — a cylindrical phase space, topologically equivalent to a solid torus.

4.2.3. Conditions for the onset of parametric chaos

Stability analysis of the linear Mathieu equation produces the Ince–Strutt diagram in the (δ, ε) parameter plane, partitioned into alternating tongue-shaped regions of stability and instability. Instability tongues — sometimes called Mathieu tongues — arise at the parametric resonance conditions:

$$\Omega \approx \frac{2\omega_0}{n}, \quad n = 1, 2, 3, \dots \quad (5)$$

Within an instability tongue the amplitude of the linear system grows without bound. When nonlinearity is present ($\alpha \neq 0$), the amplitude is bounded; however, for parameter values sufficiently deep inside the tongue the steady-state motion is no longer periodic but chaotic. The boundary of the chaotic regime in the dimensionless system is governed by:

$$\alpha > \alpha_{\text{cr}}(\delta, \varepsilon, \Omega), \quad (6)$$

$$\varepsilon > \varepsilon_{\text{cr}}(\delta, \alpha, \Omega). \quad (7)$$

For the principal resonance $n = 1$ ($\Omega \approx 2\omega_0$), with damping $\gamma \approx 0.1\omega_0$, practical threshold values are $\varepsilon_{\text{cr}} \approx 0.3\text{--}0.5$ and $\alpha_{\text{cr}} \approx 0.1\omega_0^2$. When both thresholds are exceeded, the positive Lyapunov exponent confirms the presence of deterministic chaos. The physical intuition is straightforward: the periodically modulated spring constant continuously pumps energy into the oscillation; dissipation and nonlinear saturation together fold the growing trajectory back onto itself, creating the hallmark stretching and folding mechanism of chaos.

4.2.4. Lyapunov exponent and prediction horizon

The maximum Lyapunov exponent λ_{max} quantifies the average exponential rate of divergence of initially close trajectories:

$$\lambda_{\text{max}} = \lim_{T \rightarrow \infty} \frac{1}{T} \ln \frac{|\delta \mathbf{x}(T)|}{|\delta \mathbf{x}(0)|}, \quad (8)$$

where $\delta \mathbf{x}(t)$ is the separation between two trajectories launched from states differing by $|\delta \mathbf{x}(0)| \rightarrow 0$. The system is chaotic if and only if $\lambda_{\text{max}} > 0$.

The *prediction horizon* T_{hor} is the maximum time interval over which the future state can, in principle, be forecast even with perfect knowledge of the equations of motion and near-perfect knowledge of the initial conditions:

$$T_{\text{hor}} \approx \frac{1}{\lambda_{\text{max}}} \ln \frac{\Delta_{\text{mach}}}{|\delta \mathbf{x}(0)|}, \quad (9)$$

where Δ_{mach} is the machine epsilon of the floating-point representation (approximately 10^{-16} for IEEE 754 double precision). Consider an adversary who has intercepted the transmitted waveform and,

Table 1

Recommended DPOR Parameters

Parameter	Symbol	Unit	Recommended Range	Rationale
Natural frequency	ω_0	rad/s	100–500	Compatibility with FPGA clock
Modulation frequency	Ω	rad/s	$\approx 2\omega_0$ ($\pm 5\%$)	Parametric resonance condition (5)
Modulation depth	ε	–	0.4–0.8	Above $\varepsilon_{\text{cr}} \approx 0.3$ –0.5
Nonlinearity	α	–	0.1–0.3	Above $\alpha_{\text{cr}} \approx 0.1\omega_0^2$
Damping	δ	–	0.05–0.15 ω_0	Chaos and attractor stability balance
Integration step	h	s	$\leq 0.05/\omega_0$	RK4 stability condition
Noise intensity	σ	–	10^{-4} – $10^{-3}\varepsilon$	Ergodicity without masking chaos
No. of channels	N_{ch}	–	64–1024	Jamming resistance (see Section 4.8)

by exhaustive cryptanalysis, has narrowed the initial state to $|\delta\mathbf{x}(0)| = 10^{-6}$. With $\lambda_{\text{max}} \approx 0.5 \text{ s}^{-1}$:

$$T_{\text{hor}} = \frac{1}{0.5} \ln \frac{10^{-16}}{10^{-6}} = 2 \times (-10 \ln 10) \approx -46 \text{ s}.$$

The negative value confirms that even an uncertainty of merely one part in a million in the initial conditions renders the future frequency sequence entirely unforeseeable: the adversary’s prediction error exceeds the channel spacing before a single hop has elapsed. This result is independent of the volume of intercepted signal and stands in sharp contrast to LFSR-based systems, whose state can be reconstructed deterministically from a finite intercept.

For numerical computation of λ_{max} the Wolf algorithm is employed: two trajectories separated by $|\delta\mathbf{x}(0)| = 10^{-8}$ are integrated in parallel; at each renormalisation interval T_{renorm} the deviation vector is rescaled to its initial magnitude, and the accumulated sum of logarithmic growth factors converges to λ_{max} .

4.2.5. Phase portrait and Poincaré sections

The phase portrait in the (x_1, x_2) plane and the associated Poincaré section – the discrete set of phase-plane points sampled once per excitation period $T_\Omega = 2\pi/\Omega$ – are the standard diagnostic tools for identifying the dynamical regime. Two regimes are relevant to the proposed design.

Regime I – Quasi-periodic ($\varepsilon < \varepsilon_{\text{cr}}$): The trajectory densely fills a two-dimensional invariant torus embedded in the cylindrical phase space. The Poincaré section is a smooth closed curve, a hallmark of quasi-periodicity. The Lyapunov exponent vanishes: $\lambda_{\text{max}} = 0$. The frequency sequence $\{f_k\}$ produced in this regime has a rational or irrational but structured spectrum, making it amenable to spectral analysis and ultimately predictable. This regime must be *avoided* in practice.

Regime II – Chaotic ($\varepsilon > \varepsilon_{\text{cr}}, \alpha > \alpha_{\text{cr}}$): The trajectory wanders ergodically across a *strange attractor* – a fractal set of non-integer Hausdorff dimension $d_f > 2$. The Poincaré section is a geometrically complex cloud of points exhibiting self-similar fractal structure at all observable scales. The positive Lyapunov exponent $\lambda_{\text{max}} > 0$ guarantees sensitive dependence on initial conditions. This is the operating regime exploited for PRFH generation. The ergodic property of the strange attractor is critical: it ensures that the long-run histogram of $\{x_1(t_k)\}$ converges to the attractor’s invariant measure, which in turn guarantees a statistically uniform distribution of frequency channel indices.

4.2.6. Selection of operating parameters

Based on the analysis of equations (1)–(9), Table 1 lists the recommended parameter ranges for the Digital Parametric Oscillator-Replicator (DPOR) implemented on an FPGA or DSP.

4.2.7. Formation of the discrete frequency sequence

To convert the continuous chaotic signal $x_1(t)$ into a discrete sequence of frequency channel indices $\{f_k\}$ sampled at $t_k = k T_{\text{hop}}$, a sliding statistical normalisation is applied:

$$\tilde{x}_k = \frac{x_1(t_k) - \hat{\mu}_N}{3\hat{\sigma}_N}, \quad (10)$$

where $\hat{\mu}_N$ and $\hat{\sigma}_N$ are the sample mean and standard deviation estimated over a sliding window of $N_{\text{est}} = 1000$ previous samples. The normalised signal is clipped to $[-1, +1]$ and uniformly quantised:

$$k_{\text{ch}} = \left\lfloor \frac{\tilde{x}_k + 1}{2} (N_{\text{ch}} - 1) + 0.5 \right\rfloor, \quad (11)$$

$$f_k = f_{\text{min}} + k_{\text{ch}} \Delta f, \quad (12)$$

where $\Delta f = (f_{\text{max}} - f_{\text{min}})/(N_{\text{ch}} - 1)$ is the channel spacing. Provided the attractor is ergodic and N_{est} is sufficiently large, the sample moments converge to the moments of the attractor's invariant measure, guaranteeing an asymptotically uniform distribution of channel indices. The sliding window also adapts to slow drifts in the oscillator's operating point that may arise from finite-precision arithmetic effects in long continuous runs.

4.3. Block diagram of the transceiver path

The transceiver architecture consists of two symmetric subsystems: a ground control terminal (transmitter) and an onboard receiver. Both subsystems share an identical secret parameter set loaded from a hardware-protected storage before each mission. The channel between them hops pseudo-randomly according to the chaotic frequency sequence. Figure 1 illustrates the complete block diagram with all 13 functional units; individual units are described below.

Transmit side (ground control terminal). The transmit path comprises seven functional units that together produce a frequency-agile, authenticated command waveform. Secret oscillator parameters are loaded once before the mission and never exposed in plaintext memory. The chaotic sequence is generated continuously so that a new hop frequency is always available within one integration step.

Command Packet Formatter (CPF) – unit 5. Generates a digital command packet with the following field structure: Preamble (32 bits) || UAV-ID (16 bits) || Packet Counter C_{pkt} (32 bits) || Timestamp T_{tx} (32 bits) || Command Code (16–64 bits) || MAC (32 bits) || CRC-32 (32 bits). The 32-byte Message Authentication Code (MAC) is computed with HMAC-SHA256 using a dedicated key K_{MAC} derived from the shared secret via a key derivation function (KDF), ensuring cryptographic separation between the frequency-hopping state and the authentication mechanism.

Hardware-Protected Secret Parameter Storage (HPSPS) – unit 1. A TPM or HSM module stores the initial conditions $x_0, \dot{x}_0$ and oscillator parameters $\gamma, \omega_0, \varepsilon, \Omega, \alpha$ in secure non-volatile memory. Parameters are transferred to the DPO exactly once, before the mission, through a physically secured interface, and verified by a SHA-256 hash. No plaintext copy of the parameters resides in conventional memory during operation.

Digital Parametric Oscillator (DPO) – unit 2. Implements equations (3)–(4) in double-precision (64-bit) IEEE 754 arithmetic on an FPGA or DSP processor. The integration step $h \leq 0.05/\omega_0$ ensures numerical stability and accuracy of the Runge–Kutta solver. The computation rate is $f_{\text{calc}} = 1/h \gg 1/T_{\text{hop}}$, so the oscillator state is always ready when a new hop index is needed.

Frequency Channel Quantizer-Distributor (FCQD) – unit 3. Executes the normalisation and quantisation of equations (10)–(12) in real time, maintaining the sliding statistics window. Outputs the channel index $k_{\text{ch}} \in \{0, 1, \dots, N_{\text{ch}} - 1\}$ with a guaranteed uniform distribution.

Direct Digital Synthesis Frequency Synthesizer (DDS) – unit 4. Switches the carrier frequency to f_k on command from the FCQD within $\tau_{\text{switch}} \leq 2 \text{ ms}$ (or $\leq 0.1 T_{\text{hop}}$), with a spurious-free dynamic

range of at least 60 dBc. For the upper UHF and SHF bands, a fractional- N PLL synthesiser with comparable switching time may be substituted.

Command Signal Modulator (CSM) – unit 6. Performs digital modulation – GFSK with $BT = 0.3$ or $\pi/4$ -DQPSK – and inserts guard intervals of duration $T_{\text{guard}} = 0.1 T_{\text{sym}}$ between symbols to suppress inter-symbol interference caused by transient settling after each frequency hop.

Power Amplifier and Antenna System (PA+AS) – unit 7. Provides the link energy budget. The antenna uses circular polarisation to mitigate polarisation fading over the dynamic range of UAV attitudes. The power amplifier operates in class AB for moderate efficiency with acceptable linearity for constant-envelope modulation schemes, or class E for higher efficiency with GFSK.

Receive side (onboard UAV receiver). The receive path comprises six functional units. The onboard HPSPS (marked with an asterisk in Figure 1) is a separate hardware module identical in specification to the ground-side HPSPS; it initialises the DPOR before each mission from the same shared secret.

Antenna System and Low-Noise Amplifier (AS+LNA) – unit 8. A wideband antenna – typically a microstrip patch array or low-profile monopole – covers the full hopping range $f_{\text{min}} \dots f_{\text{max}}$. The LNA has a noise figure $NF \leq 3$ dB and gain $G \geq 20$ dB. Because the antenna must remain broadband, its gain is slightly lower than for a narrowband antenna; this penalty is more than compensated by the processing gain of the PRFH system (see Section 4.8).

Synchronous Demodulator (SD) – unit 9. Down-converts the received signal to baseband (IQ demodulator) using a local oscillator locked to the current hop frequency. An automatic gain control (AGC) system with ≥ 60 dB dynamic range accommodates wide variation in received signal power. A digital phase-locked loop corrects for residual frequency offset. The synchronisation loop must acquire lock within $\leq 0.5 T_{\text{hop}}$ to leave sufficient integration time for reliable symbol detection.

Digital Parametric Oscillator-Replicator (DPOR) – unit 10. An exact hardware replica of the DPO, operating with bit-for-bit identical parameters and initial conditions. The fundamental challenge is maintaining synchronisation despite the positive Lyapunov exponent: even a perturbation as small as $|\Delta x_0| = 10^{-10}$ in the initial conditions will, after many hops, cause the DPOR trajectory to diverge from the DPO trajectory, resulting in an incorrect channel index. This requirement necessitates hardware loading of the initial state from the HPSPS with SHA-256 checksum verification, and double-precision arithmetic throughout.

Synchronisation and Offset Correction Unit (SOCU) – unit 11. Manages three synchronisation modes: (i) *Acquisition* at session start via correlative search for the Barker-13 preamble with a normalised correlation threshold $\rho_{\text{min}} = 0.8$; (ii) *Tracking* by extracting the timestamp field T_{tx} from each received packet and applying a proportional-integral correction $t_0 \leftarrow t_0 + \beta \Delta\tau$, $\beta = 0.1$, where $\Delta\tau = T_{\text{rx}} - T_{\text{tx}} - T_{\text{prop}}$; and (iii) *Re-acquisition* when $K_{\text{err}} \geq 5$ consecutive packets fail MAC or CRC verification, triggering a bidirectional index sweep of the DPOR state.

Decision Unit and Authentication Filter (DUAF) – unit 12. Implements the four-level defence described in Section 4.6.

Actuator Controller (AC) – unit 13. Converts authenticated command packets into actuator drive signals (motors, control surface servos, payload interfaces), maintains a priority command queue, and activates a Fail-Safe Return-to-Home procedure if no authenticated command is received within $T_{\text{failsafe}} \geq 2$ s.

4.4. Coupling algorithm: Chaotic sequence and command signal

The proposed method employs FFH mode with $N_{\text{FFH}} \geq 4$ hops per symbol. The hop duration is:

$$T_{\text{hop}} = \frac{T_{\text{sym}}}{N_{\text{FFH}}} = \frac{1}{R_s N_{\text{FFH}}}, \quad (13)$$

where R_s is the symbol rate in baud. At $R_s = 1200$ baud and $N_{\text{FFH}} = 4$, $T_{\text{hop}} = 208 \mu\text{s}$, corresponding to a minimum hopping rate of 4800 hops/s. Each transmitted symbol therefore occupies four distinct

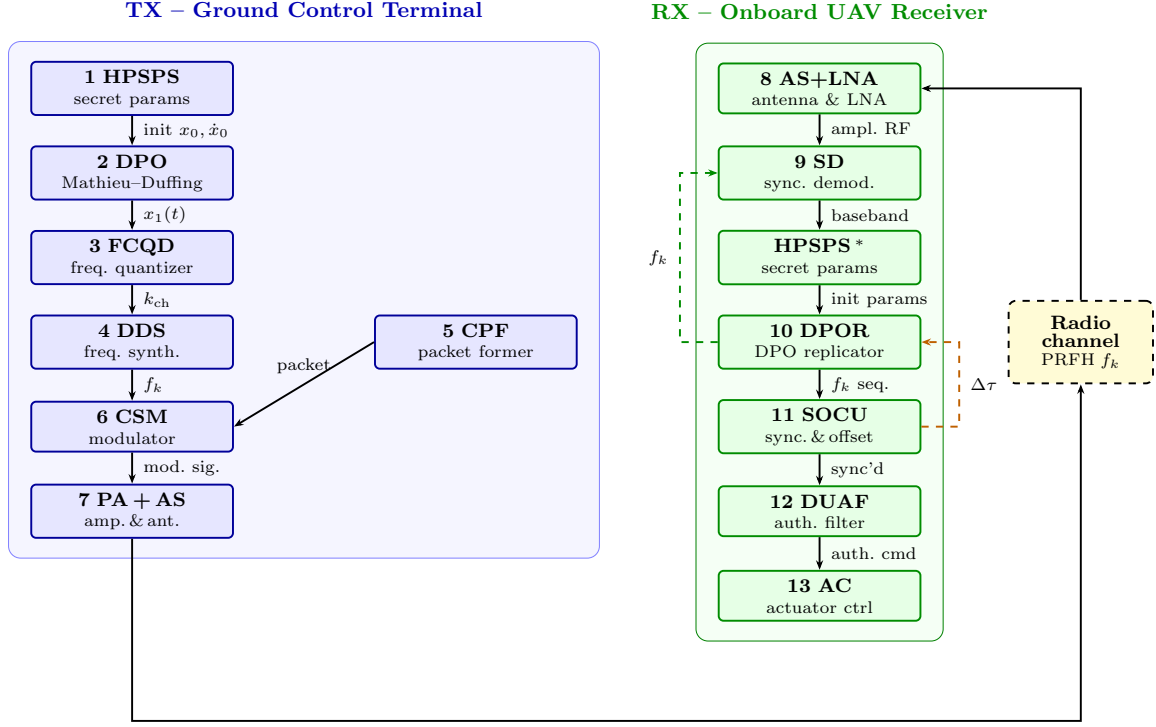


Figure 1: Block diagram of the UAV command-link transceiver with PRFH based on the Mathieu–Duffing parametric oscillator. Units 1–7 form the transmit path (ground control terminal, blue); units 8–13 form the receive path (onboard UAV receiver, green). Solid arrows denote the primary data flow; dashed arrows denote control and correction signals.

frequency slots chosen by the DPOR; no two consecutive hops carry the same channel index under normal operating conditions of the chaotic attractor.

Packet transmission proceeds in six steps.

Step 1 – Packet formation. The CPF constructs the packet: UAV-ID $\parallel C_{\text{pkt}} \parallel T_{\text{tx}} \parallel \text{CMD} \parallel \text{MAC} \parallel \text{CRC-32}$. The timestamp T_{tx} is set to the system clock value at the moment of transmission and is used by the receiver for timing synchronisation.

Step 2 – Error-correction coding. A Reed–Solomon RS(255,239) or LDPC code is applied, expanding packet length by a factor of $255/239 \approx 1.067$ and providing the ability to correct up to eight byte errors per codeword.

Step 3 – Frequency setting. The FCQD reads the current DPO state $x_1(t_k)$, computes the channel index k_{ch} via equations (10)–(12), and commands the DDS to tune to f_k . Tuning completes within $\tau_{\text{switch}} \leq 0.1 T_{\text{hop}}$, leaving at least $0.9 T_{\text{hop}}$ for energy integration at the receiver.

Step 4 – Transmission. The CSM modulates the next coded symbol and radiates it over the duration $T_{\text{sym}} = N_{\text{FFH}} T_{\text{hop}}$. Upon completion of the symbol, the DPO advances N_{FFH} integration steps and the FCQD pre-computes the next channel index so that the DDS transition is ready before the guard interval ends.

Step 5 – Synchronisation pause. A guard interval of $T_{\text{sync}} = 2 T_{\text{hop}}$ follows each packet. During this interval the SOCU measures the timing error $\Delta\tau$ and applies a correction to t_0 , so that the local DPOR clock remains aligned with the transmitter DPO clock within one integration step.

Step 6 – Acknowledgment. If a reverse channel is available, the UAV returns a short ACK packet carrying C_{pkt} to confirm delivery. A missing ACK after three consecutive retransmissions triggers a link-status alarm at the ground station.

4.5. Synchronisation and re-acquisition

Initial acquisition is performed at the start of each communication session. The transmitter sends a Barker-13 preamble $[+1, +1, +1, +1, +1, -1, -1, +1, +1, -1, +1, -1, +1]$ on a set of pre-agreed frequencies. The SOCU performs a sliding correlator search and declares acquisition when the normalised correlation exceeds $\rho_{\min} = 0.8$, establishing the timing reference t_0 .

Tracking exploits the T_{tx} field embedded in every packet. The receiver estimates the timing error:

$$\Delta\tau = T_{\text{rx}} - T_{\text{tx}} - T_{\text{prop}}, \quad (14)$$

where $T_{\text{prop}} \approx R/c$ is the one-way propagation delay (R is the current slant range, obtained from navigation telemetry or GPS). The PI correction $t_0 \leftarrow t_0 + \beta\Delta\tau$, with the damping factor $\beta = 0.1$, provides stable closed-loop tracking with adequate noise rejection.

Re-acquisition is triggered when $K_{\text{err}} \geq 5$ consecutive packets fail authentication. The SOCU enters a bidirectional index sweep: for $\Delta k = 0, +1, -1, +2, -2, \dots$ it shifts the DPOR state index by Δk hops and tests whether the next three packets are correctly authenticated. Recovery is declared upon three consecutive successful verifications. For a maximum search radius of Δk_{max} hops, the worst-case re-acquisition time is $T_{\text{rec}} \approx 2\Delta k_{\text{max}} T_{\text{pkt}}$.

4.6. Four-level authentication and interference filter

The DUAF (unit 12) implements a hierarchical decision chain. Each level provides independent rejection of illegitimate packets; a spoofed or jammed packet must defeat all four levels simultaneously to be accepted, making the overall attack probability the product of four individually small terms.

1. **Frequency gate.** A packet is accepted only if it arrives on the frequency f_k currently predicted by the DPOR. An adversary who does not know the chaotic sequence cannot concentrate interference on the correct channel. The probability that wideband interference falls by chance on the correct channel is $P_{\text{hit}} = 1/N_{\text{ch}} \leq 10^{-2}$ for $N_{\text{ch}} = 100$.
2. **Structural filter.** The packet header is verified for syntactic correctness (field lengths, magic bytes) and the UAV-ID is checked against the registered identifier.
3. **Cryptographic authentication.** The 32-byte HMAC-SHA256 tag is recomputed over the packet body and compared with the received MAC. The forgery probability is $2^{-256} \approx 10^{-77}$ per attempt, regardless of computational resources available to the adversary.
4. **Replay protection.** The packet counter C_{pkt} must be strictly greater than the last accepted value. This eliminates record-and-replay attacks in which a previously valid packet is retransmitted at a later time.

The combined probability of a successful spoofing attack — a false packet passing all four levels — is bounded by:

$$P_{\text{spoof}} \leq P_{\text{hit}} \times 2^{-256} \approx 10^{-2} \times 10^{-77} = 10^{-79}. \quad (15)$$

4.7. Comparative analysis of cryptographic strength

Table 2 compares the proposed method with three classical PRFH approaches: m-sequences, Gold codes, and nonlinear chaotic LFSRs.

The key observation from Table 2 is that the processing gain G_{fh} — which characterises jamming resistance — is identical for all four methods at the same N_{ch} . The decisive advantage of the proposed method lies entirely in its *cryptographic* properties: the sequence cannot be reconstructed from any finite intercept, and the spoofing probability is reduced by more than 70 orders of magnitude compared with m-sequences. The cost is a moderate increase in hardware complexity and a more demanding synchronisation procedure.

Table 2
Comparative Analysis of PRFH System Cryptographic Strength

Parameter	M-sequences	Gold codes	Chaotic LFSR	Proposed
Generator type	Linear LFSR	LFSR + XOR	Nonlinear LFSR	Parametric chaos
Maximum period	$2^n - 1$	$2^n - 1$	$\sim 2^{2n}$ (est.)	Practically ∞
Vulnerable to Berlekamp–Massey	Yes ($2n$ bits)	Yes ($2n$ bits)	Partially	No
Vulnerable to correlation attacks	High	Medium	Reduced	None
Intercept required for recovery	$2n$ bits	200–500 bits	$\sim 10^6$ bits	∞ (impossible)
Spoofing probability	$\sim 10^{-6}$	$\sim 10^{-6}$	$\sim 10^{-12}$	$\sim 10^{-79}$
Reproducible with same IC	Yes	Yes	Yes	Yes (det. chaos)
Synchronisation complexity	Low	Low	Moderate	High
Processing gain G_{fh} ($N_{\text{ch}} = 256$)	24 dB	24 dB	24 dB	24 dB
Hardware complexity	Low	Low	Medium	Medium–High

4.8. Link budget and jamming resistance

In a PRFH system the transmitter power is distributed uniformly across the full allocated band $\Delta f_{\text{total}} = f_{\text{max}} - f_{\text{min}}$. A jammer that concentrates all its power on a single channel can disrupt only one out of every N_{ch} hops on average; to jam all channels simultaneously it must spread its power equally, reducing its spectral power density by the processing gain:

$$G_{\text{fh}} = 10 \log_{10}(N_{\text{ch}}) \quad [\text{dB}]. \quad (16)$$

Representative values: $N_{\text{ch}} = 64 \Rightarrow G_{\text{fh}} = 18 \text{ dB}$; $N_{\text{ch}} = 256 \Rightarrow 24 \text{ dB}$; $N_{\text{ch}} = 1024 \Rightarrow 30 \text{ dB}$.

Free-space path loss follows the Friis transmission equation and is effectively constant across the hopping band provided that $\Delta f_{\text{total}}/f_c \ll 1$. The FFH mode with $N_{\text{FFH}} \geq 4$ provides frequency diversity across hops: when a single hop is corrupted by a narrowband interferer or a deep frequency-selective fade, the remaining $N_{\text{FFH}} - 1$ hops for that symbol are unaffected. A simple majority-vote decoder recovers the symbol correctly as long as fewer than $\lceil N_{\text{FFH}}/2 \rceil$ hops are erased, providing a per-symbol erasure tolerance that significantly exceeds the baseline AWGN performance.

5. Conclusions

1. A method for protecting UAV command link transmissions using PRFH based on the Mathieu–Duffing parametric oscillator has been proposed. It differs fundamentally from classical approaches by replacing algebraic LFSRs with nonlinear chaotic dynamics, eliminating the possibility of sequence reconstruction from a finite intercept.
2. The mathematical model of the chaotic regime has been developed: conditions for the onset of parametric chaos have been derived (equations (6)–(7)), an analytical expression for the prediction horizon has been established (equation (9)), and a discrete frequency sequence formation algorithm has been described (equations (10)–(12)). When the adversary’s initial-condition uncertainty is $|\delta x_0| = 10^{-6}$, the prediction horizon is negative, making every future frequency hop unforeseeable regardless of the intercept volume.
3. A complete block diagram of the transceiver path has been developed with detailed specifications for all 13 functional units and their inter-block interfaces.
4. A four-level false-packet filter has been designed — combining frequency gating, structural verification, HMAC-SHA256 authentication, and replay-counter protection — yielding an overall spoofing probability of $P_{\text{spoof}} \approx 10^{-79}$.
5. The processing gain is $G_{\text{fh}} = 10 \log_{10}(N_{\text{ch}})$, ranging from 18 to 30 dB for $N_{\text{ch}} = 64 \dots 1024$. The FFH mode ($N_{\text{FFH}} \geq 4$) provides additional frequency diversity against selective fading and narrowband jamming.

6. Future work should address: hardware-in-the-loop emulation on an SDR platform; sensitivity analysis of the DPOR to fixed-point quantisation and component tolerances; and accelerated re-acquisition algorithms for use under high-power broadband jamming.

Acknowledgments

The authors thank colleagues of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection and of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty for valuable discussions on the practical aspects of the synchronisation architecture.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] R. C. Dixon, *Spread Spectrum Systems with Commercial Applications*, 3rd ed., Wiley, New York, 1994.
- [2] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2001.
- [3] S. W. Golomb, *Shift Register Sequences*, revised ed., Aegean Park Press, Laguna Hills, CA, 1982.
- [4] W. Meier, O. Staffelbach, Fast correlation attacks on certain stream ciphers, *Journal of Cryptology* 1 (1989) 159–176. doi:10.1007/BF02252874.
- [5] J. G. Proakis, M. Salehi, *Digital Communications*, 5th ed., McGraw-Hill, New York, 2008.
- [6] Y. Liu, X. Liu, X. Mu, et al., Integrated sensing and communication for UAV systems, *IEEE Wireless Communications* 29 (2022) 36–44.
- [7] W. Khawaja, I. Guvenc, D. W. Matolak, UAS communications in BVLOS scenarios: A survey, *IEEE Access* 7 (2019) 10805–10819.
- [8] Y. Zeng, R. Zhang, T. J. Lim, Wireless communications with unmanned aerial vehicles, *IEEE Communications Magazine* 54 (2016) 36–42.
- [9] M. Ågren, C. Löndahl, M. Hell, T. Johansson, A survey on fast correlation attacks, *Cryptography and Communications* 4 (2012) 173–202. doi:10.1007/s12095-012-0062-x.
- [10] L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, *Physical Review Letters* 64 (1990) 821–824.
- [11] K. M. Cuomo, A. V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, *Physical Review Letters* 71 (1993) 65–68.
- [12] G. Kolumbán, M. P. Kennedy, L. O. Chua, The role of synchronization in digital communications using chaos, *IEEE Transactions on Circuits and Systems I* 44 (1997) 927–936.
- [13] D. J. Sobiski, J. S. Thorp, PDMA-chaos: Improved receivers for bandlimited chaotic signals, *IEEE Transactions on Circuits and Systems I* 45 (1998) 519–523.
- [14] M. Eisenkraft, et al., Chaotic synchronization in discrete-time systems connected by bandlimited channels, *IEEE Communications Letters* 15 (2011) 671–673.
- [15] A. H. Nayfeh, D. T. Mook, *Nonlinear Oscillations*, Wiley-Interscience, New York, 1979.
- [16] F. C. Moon, *Chaotic Vibrations: An Introduction for Applied Scientists and Engineers*, 2nd ed., Wiley, Hoboken, NJ, 2004.