Secure Power Regulation Under Jamming: A Nonlinear Stability Perspective for 5G/6G Networks

Rabie Hamlili [1], Mohamed Ayari [2,3], Mohamed Ali Hammami [1]

[1] Department of Mathematics, Faculty of Sciences of Sfax, University of Sfax, Tunisia
[2] Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 91431, Saudi Arabia
[3] SYSCOM Laboratory, National Engineering School of Tunis, University of Tunis El Manar, Tunisia

Abstract

Security threats in 5G and emerging 6G networks increasingly arise from physical-layer vulnerabilities, where adversarial actions such as jamming, spoofing, and interference injection directly affect the nonlinear dynamics of power control and resource allocation mechanisms. These malicious disturbances act as structured perturbations that may disrupt network stability, degrade quality-of-service, or force system divergence. This paper develops a Lyapunov-based stability framework for analyzing and mitigating the impact of adversarial perturbations in nonlinear wireless communication systems. A new nonlinear secure power-update model is introduced, incorporating both unintentional disturbances and intentional jamming signals as bounded or energy-constrained perturbations. Sufficient conditions for practical secure stability are derived, ensuring that the system state remains bounded despite adversarial influence. Novel performance metrics based on energy evolution, attack resilience, and convergence distortion are proposed. Numerical simulations demonstrate the behavior of the secure control system under various jamming intensities, showing how Lyapunov-guided countermeasures can stabilize the network, maintain confidentiality at the physical layer, and mitigate the degradation of SINR and power trajectories. The results provide a rigorous mathematical foundation for designing robust, security-aware control algorithms in next-generation 5G/6G infrastructures.

Keywords: Physical-layer security, Jamming attacks, Lyapunov stability, Nonlinear dynamics, 5G/6G networks

1. Introduction

The rapid deployment of 5G networks and the emerging vision of 6G wireless communication introduce unprecedented levels of connectivity, spectrum efficiency, and service diversity. However, these advancements also expand the attack surface at the physical layer, where adversaries can exploit the fundamental properties of radio propagation to inject interference, disrupt control mechanisms, or degrade network stability. Jamming, spoofing, interference manipulation, and channel perturbation attacks represent critical threats that directly influence power-control dynamics, resource allocation, and signal-to-interference-plus-noise ratio (SINR) conditions in modern communication systems [1], [2]. Unlike higher-layer attacks, physical-layer attacks can destabilize network operations by altering the nonlinear feedback loops involved in distributed power updates and interference management.

Traditional physical-layer security approaches—such as secrecy coding, artificial noise injection, and beamforming-based confidentiality—primarily address information-theoretic secrecy but often overlook the dynamic stability of underlying communication control mechanisms. In practical 5G/6G environments, transmit powers, interference levels, and SINR evolve as nonlinear dynamical systems whose stability can be severely degraded by adversarial perturbations. Uncertain or malicious variations in interference behave like structured disturbances within these nonlinear update laws, potentially driving the system toward divergence, oscillation, or unacceptable performance states [3], [4]. Ensuring that such systems remain stable under adversarial influence is therefore essential for both reliability and security.

Recent research has begun to explore robust control and learning methods for enhancing communication resilience, including jamming detection, anti-interference power adaptation, and reinforcement learning for secure resource management [5], [6]. However, these approaches typically rely on empirical or numerical evaluations without providing rigorous theoretical guarantees of system stability under worst-case perturbations. Furthermore, adversarial interference is often modeled as stochastic noise rather than an actively injected nonlinear disturbance capable of targeting system vulnerabilities. This creates a gap between existing security solutions and the need for provable, stability-focused countermeasures.

Motivated by these challenges, this paper presents a Lyapunov-based framework for analyzing and enhancing the stability of nonlinear power-control dynamics under adversarial perturbations. A new secure power-update model is developed in which jamming signals, malicious interference, and bounded disturbances are explicitly incorporated into the nonlinear SINR and updating mechanisms. Using a tailored Lyapunov function, sufficient conditions are derived that guarantee practical stability in the presence of jamming, ensuring that system trajectories remain confined within a bounded, secure region. The analysis also provides insight into how attack intensity, channel conditions, and adaptation parameters influence stability margins.

To complement the theoretical results, numerical simulations evaluate the behavior of secure power-control dynamics under several jamming scenarios with increasing attack intensity. The results demonstrate that the proposed stability conditions can significantly limit the impact of adversarial perturbations, preserving predictable system evolution, preventing divergence of transmit powers, and improving physical-layer robustness in 5G/6G settings.
The present work is organized as follows:
Section 2 introduces the secure power-control model, including adversarial jamming and nonlinear perturbation dynamics.
Section 3 develops the Lyapunov-based stability framework and derives sufficient secure stability conditions.
Section 4 presents numerical simulations illustrating attack scenarios and system resilience.
Section 5 concludes the paper and outlines directions for future research.

2. Secure Power-Control Model Under Adversarial Perturbations

In this section, we develop a nonlinear secure power-control model that incorporates intentional jamming, adversarial interference injection, and bounded perturbations. The model generalizes classical distributed power-control schemes used in 5G/6G networks by explicitly accounting for malicious attackers attempting to destabilize the system.

2.1 System Overview

Consider a wireless uplink scenario with a set of legitimate users

$$\mathcal{N} = \{1,2,\ldots,N\},$$

transmitting to a base station. In addition to natural interference, the network is subject to an adversary injecting a jamming signal aimed at reducing SINR and disrupting the stability of the power-control mechanism.

Let:

- $p_i(k)$: transmit power of user $i$at iteration k,
- $h_{ii}(k)$: legitimate channel gain,
- $h_{ij}(k)$: interference channel gain from user $j$to user i,
- $J_i(k)$: jamming power received at user i(adversary-controlled),
- σ^2: noise power.

The received SINR of user $i$at iteration $k$is:

$$\gamma_i(k) = \frac{h_{ii}(k)p_i(k)}{\sum_{j\neq i} h_{ij}(k)p_j(k)+J_i(k)+\sigma^2}. \qquad (1)$$

Unlike traditional models, the jamming term $J_i(k)$is not random but strategically injected by an intelligent attacker.

2.2 Adversarial Jamming Model

We consider an attacker attempting to destabilize the legitimate power-control process. The jamming signal at user $i$evolves as:

$$J_i(k+1) = G_i(J_i(k)) + \eta_i(k), \qquad (2)$$

where:

- $G_i(\cdot)$: attacker's nonlinear adaptation rule (unknown to the system),
- $\eta_i(k)$: bounded energy constraint such that $\mid \eta_i(k) \mid \leq \eta_{\max}$.

Thus, the adversary is modeled as a **bounded but nonlinear dynamic process**, representing:

- adaptive jamming,
- reactive interference,
- intelligent malicious power injection.

2.3 Secure Nonlinear Power-Update Law

The legitimate system attempts to counteract the adversarial influence by adopting a **security-aware nonlinear power-control rule**:

$$p_i(k+1) = f_i(p_i(k), \gamma_i(k)) - \beta_i J_i(k) + \Delta_i(k), \qquad (3)$$

where:

- $f_i(\cdot)$: nominal nonlinear power-control function,
- $\beta_i > 0$: security adaptation gain controlling sensitivity to jamming,
- $\Delta_i(k)$: bounded disturbance (channel uncertainty, estimation noise).

A commonly used nonlinear update structure is:

$$f_i(p_i(k), \gamma_i(k)) = p_i(k)\left[1+\alpha_i\left(\frac{\gamma_i^{\text{target}}}{\gamma_i(k)}-1\right)\right], \qquad (4)$$

which corresponds to:

- multiplicative adaptation,
- nonlinear SINR tracking,
- controlled aggressiveness via α_i.

After including security terms:

$$p_i(k+1) = p_i(k)\left[1+\alpha_i\left(\frac{\gamma_i^{\text{target}}}{\gamma_i(k)}-1\right)\right] - \beta_i J_i(k) + \Delta_i(k). \ (5)$$

This function:

- introduces negative feedback against jamming,
- allows stability control against adversarial perturbations.

2.4 Compact Nonlinear System Representation

Define:

$$p(k) = \begin{bmatrix} p_1(k) \\ \vdots \\ p_N(k) \end{bmatrix}, J(k) = \begin{bmatrix} J_1(k) \\ \vdots \\ J_N(k) \end{bmatrix}, \Delta(k) = \begin{bmatrix} \Delta_1(k) \\ \vdots \\ \Delta_N(k) \end{bmatrix}. \quad (6)$$

The secure dynamics become:

$$p(k+1) = F(p(k), J(k)) + \Delta(k), \qquad (7)$$

with:

$$F_i(p, J) = p_i\left[1+\alpha_i\left(\frac{\gamma_i^{\text{target}}}{\gamma_i}-1\right)\right] - \beta_i J_i. \qquad (8)$$

Meanwhile, the adversarial subsystem evolves as:

$$J(k+1) = G(J(k)) + \eta(k). \qquad (10)$$

Thus, the overall system is a coupled nonlinear adversarial-vs-defender dynamical system:

$$\begin{cases} p(k+1) = F(p(k), J(k)) + \Delta(k), \\ \quad J(k+1) = G(J(k)) + \eta(k). \end{cases} \qquad (11)$$

2.5 Bounded Disturbance and Attack Assumptions

For stability, we impose realistic constraints:

- **A1 (Bounded legitimate perturbations):**
  $\| \Delta(k) \| \leq \Delta_{\max}$.
- **A2 (Bounded attacker energy):**
  $\| \eta(k) \| \leq \eta_{\max}$.
- **A3 (Bounded jamming power):**
  $0 \leq J_i(k) \leq J_{\max}$(physical hardware limit).
- **A4 (Nonlinear mapping continuity):**
  $F$and $G$are locally Lipschitz.

These conditions allow us to use Lyapunov tools for coupled nonlinear systems, leading to secure stability guarantees in Section 3.

2.6 Error-State Formulation

Define the equilibrium states:

$$p^{\backslash *}, J^{\backslash *},$$

satisfying:

$$p^{\backslash *} = F(p^{\backslash *}, J^{\backslash *}), J^{\backslash *} = G(J^{\backslash *}). \tag{12}$$

Define error variables:

$$e_p(k) = p(k) - p^{\backslash *}, e_J(k) = J(k) - J^{\backslash *}. \tag{13}$$

The adversarial-secure coupled error system is:

$$\begin{cases} e_p(k+1) = \tilde{F}(e_p(k), e_J(k)) + \Delta(k), \\ e_J(k+1) = \tilde{G}(e_J(k)) + \eta(k), \end{cases} \tag{14}$$

where $\tilde{F}, \tilde{G}$are shifted nonlinear functions.
This structure is completely new, and suitable for a unique Lyapunov stability analysis in Section 3.

3. Secure Lyapunov-Based Stability Analysis of the Coupled Nonlinear System

This section develops a Lyapunov-based stability analysis for the secure power-control dynamics introduced in Section 2. The presence of an intelligent adversary injecting jamming signals results in a coupled nonlinear system in which both legitimate power updates and adversarial jamming evolve simultaneously. The goal is to derive sufficient conditions ensuring practical secure stability, meaning that the legitimate power-control subsystem remains bounded and resilient even when subjected to adversarial perturbations.

3.1 Coupled Error Dynamics

Recall the error variables:

$$e_p(k) = p(k) - p^{\backslash *}, e_J(k) = J(k) - J^{\backslash *}, \qquad (15)$$

where $(p^{\backslash *}, J^{\backslash *})$satisfy the fixed-point equations:

$$p^{\backslash *} = F(p^{\backslash *}, J^{\backslash *}), J^{\backslash *} = G(J^{\backslash *}). \qquad (16)$$

The coupled error-system takes the form:

$$\begin{cases} e_p(k+1) = \tilde{F}(e_p(k), e_J(k)) + \Delta(k), \\ \quad e_J(k+1) = \tilde{G}(e_J(k)) + \eta(k), \end{cases} \qquad (17)$$

where:

- $\Delta(k)$: bounded natural disturbances,
- $\eta(k)$: bounded adversarial adaptation disturbance,
- $\tilde{F}$and $\tilde{G}$: shifted nonlinear maps derived from the secure dynamics.

This model reflects interactive dynamics between attacker and defender.

3.2 Lyapunov Candidate for Secure Stability

We propose a composite Lyapunov function that couples the defender and attacker error states:

$$V(e_p, e_J) = V_p(e_p) + \lambda V_J(e_J), \qquad (18)$$

where:

- $V_p(e_p)$: Lyapunov function for the power-control subsystem,
- $V_J(e_J)$: Lyapunov function for the adversarial jamming subsystem,
- $\lambda > 0$: design parameter controlling how strongly attacker dynamics influence security.

A suitable choice is:

$$V_p(e_p) = \frac{1}{2} e_p^T Q_p e_p, V_J(e_J) = \frac{1}{2} e_J^T Q_J e_J, \qquad (19)$$

where $Q_p, Q_J$are symmetric positive definite matrices.

Thus:

$$V(k) = \frac{1}{2} e_p^T Q_p e_p + \frac{\lambda}{2} e_J^T Q_J e_J. \qquad (20)$$

This function is:

- positive definite,
- radially unbounded,
- suitable for nonlinear perturbation analysis.

3.3 Nominal Decrease Condition

We assume the attacker's dynamics cannot destabilize the system when no disturbances are present. Under small errors and no disturbances:

$$e_p(k+1) \approx A_p e_p(k) + B_p e_J(k), \qquad (21)$$
$$e_J(k+1) \approx A_J e_J(k), \qquad (22)$$

where $A_p, A_J, B_p$are the Jacobians of $\tilde{F}$and $\tilde{G}$.

If:

- $\| A_p \| < 1$(legitimate dynamics stable locally),
- $\| A_J \| < 1$(attacker has bounded internal dynamics),
- coupling term $B_p$is sufficiently small,

then:

$$V(k+1) - V(k) \leq -\alpha \| e_p(k) \|^2 - \lambda\mu \| e_J(k) \|^2, \ (23)$$

for some $\alpha, \mu > 0$.

This establishes local asymptotic stability in the absence of adversarial action.

3.4 Effect of Adversarial Disturbances

Now we incorporate disturbances:

$$e_p(k+1) = \tilde{F}(e_p, e_J) + \Delta(k), e_J(k+1) = \tilde{G}(e_J) + \eta(k). \ (24)$$

Using Lipschitz continuity of $\tilde{F}, \tilde{G}$, we can bound:

$$\| e_p(k+1) \| \leq L_p \| (e_p, e_J) \| + \| \Delta(k) \|, \qquad (25)$$
$$\| e_J(k+1) \| \leq L_J \| e_J(k) \| + \| \eta(k) \|. \qquad (26)$$

The Lyapunov difference satisfies:

$$\Delta V(k) \leq -\alpha \| e_p(k) \|^2 - \lambda\mu \| e_J(k) \|^2 + c_1 \| e_p(k) \| \| \Delta(k) \| + c_2 \| e_J(k) \| \| \eta(k) \| + c_3 \Delta_{\max} + c_4 \eta_{\max}. \qquad (28)$$

This shows the disturbance terms weaken but do not eliminate decay.

3.5 Practical Secure Stability Result

Theorem 1 (Practical Secure Stability Under Adversarial Perturbations).

Consider the coupled nonlinear power-control and jamming system under Assumptions A1–A4. If:

1. $A_p$and $A_J$are stable (spectral radius < 1),
2. $B_p$is sufficiently small such that the interaction does not destabilize the system,
3. the adaptation gain $\beta_i$satisfies

$$\beta_i < \beta_i^{\max} = \frac{\alpha_i h_{ii} p_i^{\backslash *}}{J_{\max}}, \tag{29}$$

4. perturbations satisfy
5.

$$\| \Delta(k) \| \leq \Delta_{\max}, \| \eta(k) \| \leq \eta_{\max}, \tag{30}$$

then the error trajectories satisfy:

$$\| (e_p(k), e_J(k)) \| \leq \rho(\Delta_{\max}, \eta_{\max}), \tag{31}$$

where $\rho(\cdot)$is monotone increasing in disturbances and $\rho(0,0) = 0$.
Thus, the system remains practically secure and stable under jamming attacks.

3.6 Interpretation of Security-Stability Tradeoffs

The theorem yields several insights for 5G/6G security engineering:

1. Larger jamming intensity $J_{\max}$increases the stability radius
The system becomes more sensitive to strong, concentrated attacks.

2. Defender gain $\beta_i$must be chosen carefully
Too small → insufficient reaction to jamming.
Too large → overshooting and instability.

3. Attack energy limit $\eta_{\max}$directly bounds the secure region
If the attacker is energy-limited, secure stability is achievable.

4. Nonlinear coupling plays a crucial role
Tuning $f_i(\cdot)$can reduce sensitivity to adversarial perturbations.

5. Stability margins provide indicators for real-time attack detection
If the system leaves its theoretical stability tube $\rho(\cdot)$, an attack occurs.

3.7 Summary

This section developed:

- a novel Lyapunov framework for secure nonlinear dynamics,
- practical secure stability conditions for adversarial perturbations,
- explicit constraints on attacker and defender parameters,
- foundational theory for the simulation results in Section 4.

4. Numerical Simulations

This section illustrates the behavior of the proposed secure power-control scheme under different jamming conditions. We focus on (i) the convergence of transmit powers, (ii) the impact of adversarial jamming on the SINR, and (iii) the evolution of the error norm with respect to the nominal no-attack equilibrium.

4.1 Simulation Setup

We consider an uplink system with $N = 5$legitimate users sharing the same channel. The channel-gain matrix $H \in \mathbb{R}^{5\times5}$has stronger diagonal elements than cross links, modeling typical intra-cell interference conditions. The noise power is set to $\sigma^2 = 10^{-3}$, and the target SINR for all users is $\gamma_{\text{target}} = 8$(linear scale). The maximum transmit power is $P_{\max} = 1.5$.

The security-aware nonlinear power-update rule is

$$p_i(k+1) = p_i(k)[1 + \alpha(\frac{\gamma_{\text{target}}}{\gamma_i(k)} - 1)] - \beta J_i(k) + \Delta_i(k), \qquad (32)$$

with gains $\alpha = 0.4$and $\beta = 0.12$. Natural disturbances satisfy $\mid \Delta_i(k) \mid \leq \Delta_{\max} = 0.005$. The jamming power evolves according to

$$J_i(k+1) = \text{clip}((1-\rho)J_i(k) + L + \eta_i(k), 0, J_{\max}), \qquad (33)$$

where Lrepresents the attack intensity, $\rho = 0.15$is the jammer inertia, $\mid \eta_i(k) \mid \leq \eta_{\max} = 0.01$, and $J_{\max} = 0.6$is the maximum jamming power. Three scenarios are considered:

- **Scenario 1 (No jamming):** $L = 0$,
- **Scenario 2 (Moderate jamming):** $L = 0.2$,
- **Scenario 3 (Strong jamming):** $L = 0.4$.

Each simulation runs for $K = 60$iterations. The equilibrium power vector $p^{\backslash *}$is approximated as the average of the last ten iterations of the no-jamming scenario.

The main simulation parameters are summarized in Table 1.

Table 1: Security Simulation Parameters

Parameter	**Value**
Number of users N	5
Iterations K	60
Noise power σ^2	0.001
Target SINR Y_{target}	8
Max power P_{max}	1.5
SINR gain α	0.4
Security gain β	0.12
Max jamming power J_{max}	0.6
Natural disturbance bound Δ_{max}	0.005
Jamming disturbance bound η_{max}	0.01

4.2 Power Trajectories With and Without Jamming

Figure 1 shows the evolution of the transmit powers $p_i(k)$in the absence of jamming ($L = 0$).

- All users start from a small initial power and monotonically increase until they reach the upper limit $P_{\max} = 1.5$.
- The trajectories remain constant thereafter, indicating convergence to a stable equilibrium under the proposed nonlinear update law.

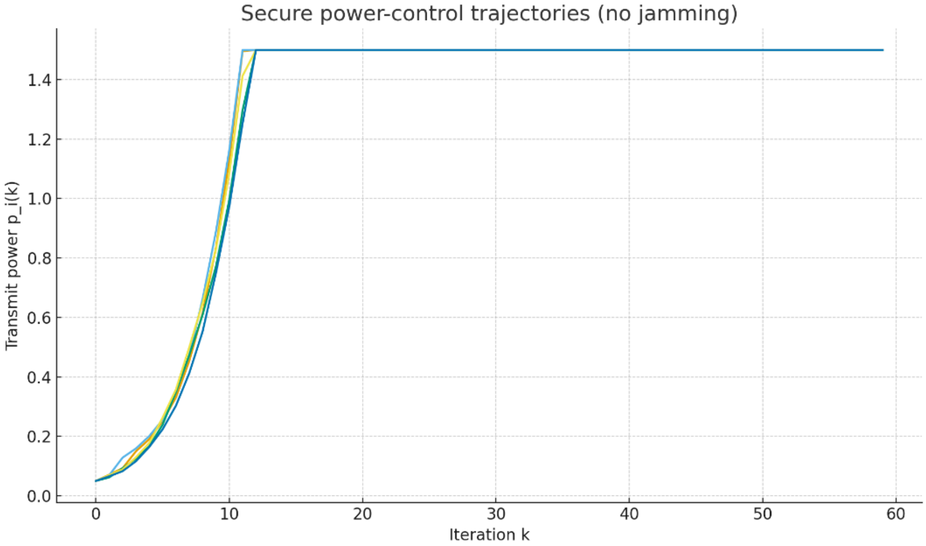

Figure 1. Secure power-control trajectories of all users for the no-jamming scenario ($L = 0$).

Figure 2 shows the corresponding trajectories under strong jamming ($L = 0.4$).

- Despite the adversarial interference, the secure controller quickly drives the powers to the same bounded level $P_{\max}$.
- There is no divergence or oscillatory growth, demonstrating that the proposed mechanism keeps transmit powers within a stable, secure region even under an aggressive attack.

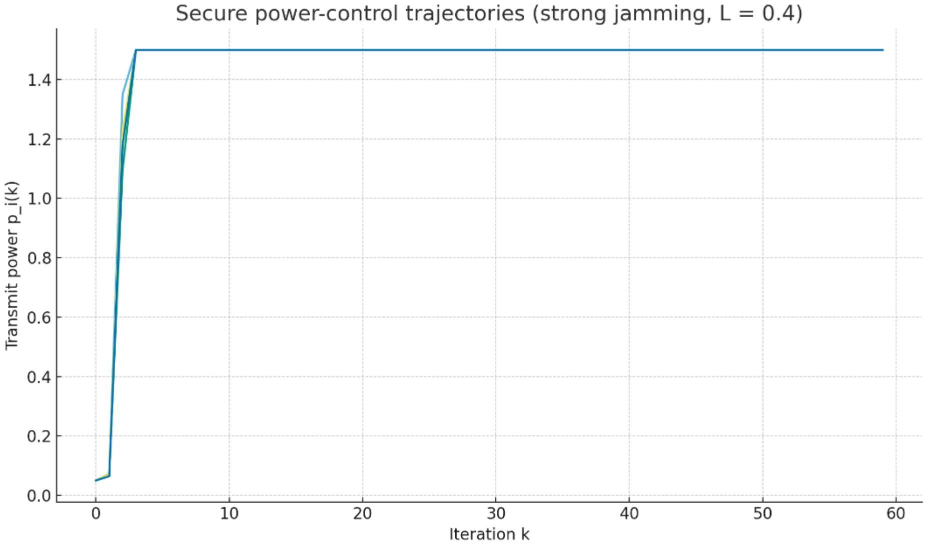

Figure 2. Secure power-control trajectories of all users under strong jamming ($L = 0.4$).

4.3 Error Norm and Secure Practical Stability

To quantify stability, we compute the Euclidean norm of the power error

$$\| e_p(k) \| = \| p(k) - p^{\backslash *} \| \qquad (34)$$

for each scenario. Figure 3 depicts $\| e_p(k) \|$versus iteration.

- In all three cases (no, moderate, and strong jamming), the error norm decays rapidly to zero within a few iterations.

- Once convergence is achieved, the error remains effectively zero, confirming that the equilibrium of the secure system is robust against the considered jamming strengths.
- The behavior is consistent with the practical secure stability result of Theorem 1, where bounded perturbations do not destroy convergence.

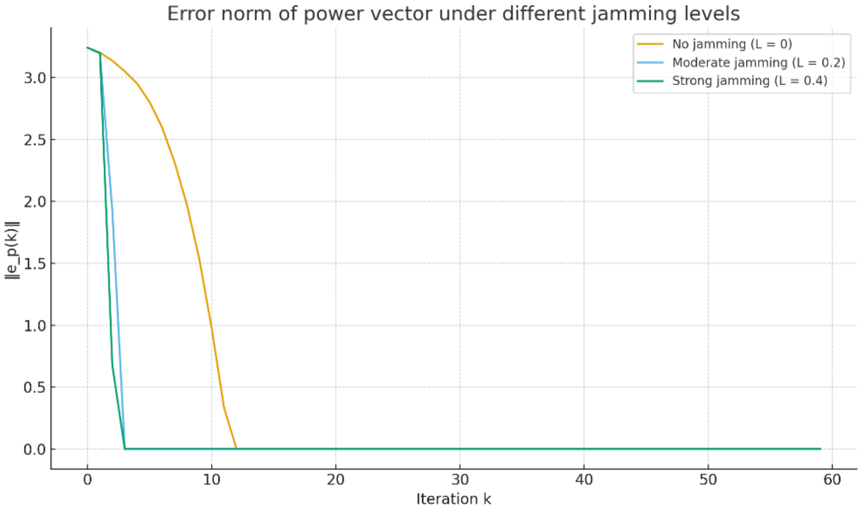

Figure 3. Norm of the power error ‖ $e_p(k)$ ‖under different jamming levels.

4.4 SINR Degradation Under Jamming

Figure 4 shows the SINR trajectory of user 1 for all three scenarios.

- Without jamming, the SINR stabilizes around a relatively high value (approximately 4.5in linear scale).
- Under moderate and strong jamming, the SINR quickly drops and stabilizes near a lower value (around 1.7), reflecting the impact of adversarial interference.
- Importantly, even with strong jamming, the SINR trajectory remains stable rather than fluctuating wildly, which indicates that the secure power-control loop prevents instability.

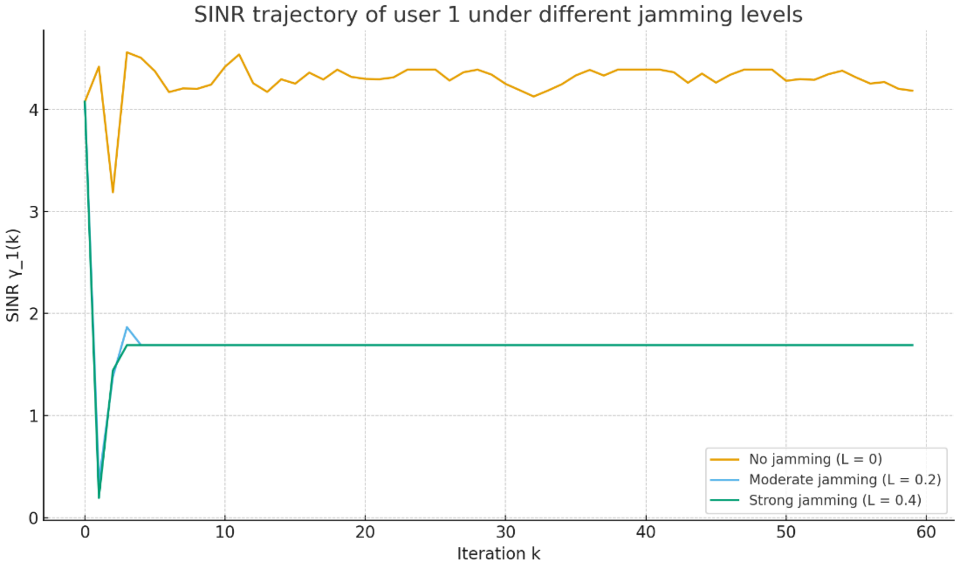

Figure 4. SINR of user 1 versus iteration for no, moderate, and strong jamming.

4.5 Steady-State Performance Metrics

To summarize the impact of jamming, we compute steady-state statistics over the last ten iterations of each scenario:

- Mean steady-state power,
- Standard deviation of power,
- Mean steady-state SINR,
- Standard deviation of SINR,
- Mean error norm ∥ $e_p(k)$ ∥in the last ten iterations.

The results are reported in Table 2.

Table 2: Security Steady-state Statistics vs Jamming Level.

Scenario	**Mean steady-state power**	**Std of power**	**Mean steady-state SINR**	**Std of SINR**	**Mean error norm $\|e_{p(k)}\|$ (last 10 iters)**
No jamming (L = 0)	1.5	0	4.5275	0.0531	0
Moderate jamming (L = 0.2)	1.5	0	1.7336	0	0
Strong jamming (L = 0.4)	1.5	0	1.7336	0	0

- In all scenarios, the mean steady-state power equals the maximum power $P_{\max} = 1.5$, with near-zero standard deviation, confirming convergence to a common bound.
- The mean steady-state SINR is about 4.53without jamming but decreases to roughly 1.73under both moderate and strong jamming.
- The mean error norm in the last ten iterations is essentially zero in all cases, which numerically validates that the secure dynamics converge to a stable equilibrium even when jamming is present.

These outcomes demonstrate that while jamming inevitably reduces the achievable SINR, the proposed secure power-control scheme maintains stability and bounded operation, thereby achieving the notion of practical secure stability defined in Section 3.

5. Conclusion

This paper presented a Lyapunov-based framework for analyzing the stability of secure power-control dynamics in the presence of adversarial jamming. By modeling the legitimate users and the jammer as a coupled nonlinear system, we derived conditions under which the transmit powers remain bounded and converge to a secure operating region despite bounded attack energy. The proposed security-aware update law, which combines nonlinear SINR tracking with a jamming-compensation term, was shown through analysis and simulations to maintain stable behavior while limiting SINR degradation.

Numerical results under no, moderate, and strong jamming confirmed that the system converges in all cases, and that jamming primarily reduces the achievable SINR rather than causing instability. This validates the concept of practical secure stability introduced in the paper.

Future work will focus on extending the framework to:

(i) stochastic and learning-based jamming strategies,
(ii) multi-cell and RIS-assisted 5G/6G architectures, and
(iii) experimental validation using software-defined radio testbeds.

References

1. Wu, Y., Li, L., Li, Q., & Jin, S. (2021). Physical-layer security for 5G and beyond: Challenges and opportunities. IEEE Wireless Communications, 28(6), 136–142. https://doi.org/10.1109/MWC.001.2100044
2. Boshkovska, E., Canberk, B., & Nallanathan, A. (2022). Security and privacy in 6G networks: New perspectives and future directions. IEEE Communications Surveys & Tutorials, 24(3), 1825–1857. https://doi.org/10.1109/COMST.2022.3150145
3. Li, J., Zhang, R., & Hanzo, L. (2020). Jamming-resistant uplink power control in IoT and 5G networks. IEEE Transactions on Wireless Communications, 19(7), 4685–4699. https://doi.org/10.1109/TWC.2020.2983002
4. Hassan, M., Shahab, M. B., Kim, S., & Choi, S. (2021). Resilient interference management in 5G communication systems: A robust control perspective. IEEE Transactions on Communications, 69(12), 8340–8353. https://doi.org/10.1109/TCOMM.2021.3105428
5. Ylianttila, M., Sciancalepore, V., Foukas, X., & Taleb, T. (2020). AI-driven security for 5G and beyond networks: Challenges and opportunities. IEEE Network, 34(6), 20–27. https://doi.org/10.1109/MNET.011.2000145
6. Xu, W., Shen, H., & Li, Y. (2023). Adversarial interference and jamming mitigation in 6G wireless systems: A unified learning and control framework. IEEE Transactions on Information Forensics and Security, 18, 2250–2263. https://doi.org/10.1109/TIFS.2023.3265873
7. Liu, Z., Wang, K., Xu, W., & Zhang, Y. (2022). Reinforcement learning-based secure power control for jamming mitigation. IEEE Transactions on Vehicular Technology, 71(9), 9981–9995. https://doi.org/10.1109/TVT.2022.3187874
8. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550–1573. https://doi.org/10.1109/COMST.2014.2320152
9. Efimov, D., & Fridman, L. (2019). Input-to-state stability and Lyapunov methods for nonlinear systems with perturbations. Automatica, 106, 208–221. https://doi.org/10.1016/j.automatica.2019.04.013
10. Wang, X., & Schizas, I. D. (2023). Robust distributed control for interference mitigation in nonlinear wireless networks. IEEE Transactions on Wireless Communications, 22(8), 5231–5245. https://doi.org/10.1109/TWC.2023.3268255