Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Detection and Suppression of Malicious Perturbations in Nonlinear Lattice Networks: A Security-Oriented Frenkel–Kontorova Framework

Dalel Amri[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

The Frenkel–Kontorova (FK) model, traditionally used to describe nonlinear interactions in atomic chains and structured materials, has emerging relevance in 6G communication platforms and metasurface-based architectures. However, these lattice-like structures may be vulnerable to malicious perturbations, targeted interference, or adversarial manipulation, which can destabilize wave propagation and compromise physical-layer security. This paper introduces a security-oriented FK framework for modeling, detecting, and mitigating adversarial disturbances in nonlinear lattice networks. A perturbed FK system is constructed in which the attacker injects structured, spatially correlated disturbances designed to distort lattice synchronization, disrupt soliton propagation, or alter equilibrium configurations. A novel detection mechanism based on deviation energy, lattice tension metrics, and spatiotemporal anomalies is proposed, along with a stability suppression strategy using adaptive damping and nonlinear compensation. Lyapunov and energy-based analyses are used to derive sufficient conditions for disturbance detectability and secure lattice stabilization. Numerical simulations demonstrate the model's ability to identify malicious perturbations, quantify attack intensity, and restore stable wave patterns through lattice-level corrective mechanisms. The results highlight the potential of FK-based modeling as a foundational tool for enhancing physical-layer security in future 6G metasurfaces, nano-resonator arrays, and programmable communication structures.

Keywords: Frenkel–Kontorova model, Security perturbations, Nonlinear lattices, 6G metasurfaces, Stability analysis

1. Introduction

Structured lattice systems play an increasingly important role in next-generation wireless technologies, particularly in the development of reconfigurable intelligent surfaces (RIS), programmable metasurfaces, and nano-resonator arrays envisioned for 6G networks. These artificial structures manipulate electromagnetic waves through coordinated interactions among tightly coupled elements arranged in

periodic or quasi-periodic patterns. Because of their geometric and dynamic similarity to nonlinear lattice models, frameworks such as the Frenkel–Kontorova (FK) system have emerged as powerful analytical tools for studying wave propagation, synchrony, localized excitations, and nonlinear energy transfer within these engineered surfaces [1], [2]. The FK model is especially useful in capturing the behavior of spatially coupled oscillators subjected to periodic potentials, enabling a rigorous characterization of solitons, kinks, and dynamic regimes relevant to programmable lattice-based communication architectures.

As 6G technologies move toward highly controllable and software-programmable surfaces, security challenges arise at the physical and structural levels of the lattice itself. Adversaries may seek to exploit the dynamic properties of metasurfaces or RIS structures by injecting malicious perturbations, altering element responses, desynchronizing oscillator phases, or causing controlled distortions in wave-front shaping. These lattice-level manipulations can compromise system integrity, degrade communication performance, and enable advanced physical-layer attacks such as beam misdirection, covert channel creation, or RIS hijacking [3], [4]. Because metasurfaces often rely on dense, tightly coupled arrays, localized perturbations can propagate through the lattice, amplifying attack effects and making the overall system vulnerable to structural destabilization.

Recent studies on metasurface and RIS security have focused on signal-level threats, unauthorized configuration changes, and machine-learning-based attack detection [5], [6]. However, little attention has been given to lattice-dynamic vulnerabilities, where malicious forces or perturbations are introduced directly at the physical layer of the structure. The FK model provides a natural foundation for analyzing these threats because it explicitly captures how local disruptions propagate across neighboring nodes through nonlinear coupling. Moreover, the inherent energy structure of the FK lattice allows for the construction of security metrics that quantify abnormal tension, wave distortion, or deviation from equilibrium, forming the basis of anomaly detection and stabilization strategies.

Motivated by these considerations, this paper introduces a security-oriented Frenkel–Kontorova framework designed to detect and suppress malicious perturbations in nonlinear lattice networks. A perturbed FK model is formulated in which adversarial disturbances take the form of spatially structured or time-varying injections intended to destabilize the lattice or distort its wave propagation characteristics. Building on this model, we develop an anomaly detection scheme based on deviation energy, lattice-stress measures, and spatiotemporal irregularities. Furthermore, an adaptive stabilization mechanism is proposed that counteracts adversarial effects using nonlinear compensation and adjustable damping. Lyapunov and energy-based analyses establish conditions for the detectability and boundedness of perturbations, ensuring that the lattice remains stable under attack.

The present work is organized as follows: Section 2 introduces the malicious-perturbation FK model and describes the adversarial and defensive mechanisms. Section 3 develops detection metrics and provides Lyapunov-based secure stability analysis. Section 4 presents numerical simulations demonstrating detection accuracy, attack propagation, and stabilization effectiveness. Section 5 concludes the paper and highlights future directions for FK-based physical-layer security.

2. Malicious Perturbation Model for Frenkel–Kontorova Lattices

To analyze how adversarial disturbances affect structured communication surfaces and nonlinear lattice networks, we extend the classical Frenkel–Kontorova (FK) model to incorporate malicious perturbations, structured attack injections, and defensive stabilization mechanisms. This section introduces the dynamic equations for the perturbed lattice, the attacker's strategy, and the defender's countermeasure actions.

2.1 Baseline FK Lattice Dynamics

Let $u_n(t)$denote the displacement (or phase / meta-atom state) of the n-th element in a nonlinear lattice. The standard continuous-time FK model is:

$$m\ddot{u}_n + \alpha\dot{u}_n + V'(u_n) + K(u_n - u_{n-1}) + K(u_n - u_{n+1}) = F_n(t), \quad (1)$$

where:

- m— mass or inertia parameter,
- α— damping coefficient,
- K— coupling strength between neighboring sites,
- $V(u)$— periodic substrate potential, usually

$$V(u) = \frac{V_0}{(2\pi)^2}(1 - \cos(2\pi u)), V'(u) = \frac{V_0}{2\pi}\sin(2\pi u), \quad (2)$$

- $F_n(t)$— external forcing (benign or malicious).

The FK model is widely used to describe wave propagation, soliton motion, and nonlinear interactions in engineered lattice systems.

2.2 Malicious Perturbation Injection Model

To represent a physical-layer attack, we assume an adversary injects malicious perturbations into selected lattice nodes.

Let:

$$F_n(t) = F_n^{(0)}(t) + A_n(t), \quad (3)$$

where:

- $F_n^{(0)}(t)$— legitimate external driving (e.g., control or signal shaping),
- $A_n(t)$— *adversarial force* applied to the lattice.

We model the attack term as:

$$A_n(t) = \psi_n(t) + \zeta_n(t), \quad (4)$$

where:

- $\psi_n(t)$— structured, coordinated attack (e.g., periodic, resonant, or spatially correlated),
- $\zeta_n(t)$— bounded random perturbation (noise-like malicious activity).

Example structured attack patterns

1. **Targeted node attack (localized)**

$$\psi_n(t) = A_0 \sin(\omega t)\, \delta_{n,k_0}, \tag{5}$$

attacking node k_0.

2. **Spatial wave attack**

$$\psi_n(t) = A_0 \sin(\omega t - qn), \tag{6}$$

disrupting wavefronts.

3. **Desynchronization attack**

$$\psi_n(t) = A_0\, \mathrm{sgn}(u_{n-1}(t) - u_{n+1}(t)), \tag{7}$$

promoting phase mismatch between neighbors.

2.3 Defender Stabilization Mechanism

To counteract malicious perturbations, we introduce a defensive correction force $D_n(t)$applied by a lattice controller:

$$D_n(t) = -\beta_1 \dot{u}_n(t) - \beta_2(2u_n(t) - u_{n-1}(t) - u_{n+1}(t)), \tag{8}$$

where:

- β_1— adaptive damping gain,
- β_2— corrective coupling gain.

This defender mechanism:

- increases local damping when a disturbance is detected,
- counteracts divergence tendencies,
- re-synchronizes neighboring nodes,
- smooths malicious wave propagation.

2.4 Complete Security-Oriented FK Model

Combining the baseline dynamics, the malicious force, and the defense mechanism:

$$m\ddot{u}_n + (\alpha + \beta_1)\dot{u}_n + V'(u_n) + (K + \beta_2)(2u_n - u_{n-1} - u_{n+1}) = F_n^{(0)}(t) + \psi_n(t) + \zeta_n(t). \tag{9}$$

Define the effective parameters:

- Effective damping:

$$\alpha_{\text{eff}} = \alpha + \beta_1, \tag{10}$$

- Effective coupling:

$$K_{\text{eff}} = K + \beta_2. \tag{11}$$

Thus, the closed-loop secure FK system becomes:

$$m\ddot{u}_n + \alpha_{\text{eff}}\dot{u}_n + V'(u_n) + K_{\text{eff}}(2u_n - u_{n-1} - u_{n+1}) = F_n^{(0)}(t) + \psi_n(t) + \zeta_n(t). \tag{12}$$

2.5 Discrete-Time Approximation for Attack Detection & Stability

For numerical simulations and stability analysis, use:

$$u_n(k+1) = u_n(k) + h\, v_n(k), \tag{13}$$

$$v_n(k+1) = v_n(k) + h[-\tfrac{\alpha_{\text{eff}}}{m} v_n(k) - \tfrac{1}{m} V'(u_n(k)) - \tfrac{K_{\text{eff}}}{m}(2u_n(k) - u_{n-1}(k) - u_{n+1}(k)) + \tfrac{1}{m} A_n(k)]. \tag{14}$$

This discrete representation enables:

- attack detection (energy deviation, tension metrics),
- Lyapunov stability analysis,
- simulation of attack propagation,
- evaluation of defensive strategies.

2.6 Security-Relevant Signals

To support detection and stability later, define:

Lattice tension (attack-sensitive metric)

$$T_n(k) = | u_n(k) - u_{n-1}(k) |. \tag{15}$$

Sharp increases indicate perturbation.

Deviation energy

$$E_{\text{dev}}(k) = \sum_n \left[\tfrac{1}{2} m v_n^2 + \tfrac{K_{\text{eff}}}{2}(u_n - u_{n-1})^2\right]. \tag{16}$$

Useful for anomaly detection.

3. Detection Metrics and Secure Stability Analysis

This section introduces analytic tools for detecting malicious perturbations in nonlinear FK lattices and for establishing practical stability under adversarial disturbances. We develop (i) anomaly indicators based on lattice tension and deviation energy, and (ii) a Lyapunov-based framework that quantifies the resilience of the lattice dynamics in the presence of coordinated attacks.

3.1 Detection Metrics for Malicious Perturbations

Malicious perturbations tend to disrupt the regular spatiotemporal pattern of lattice motion. To detect these abnormalities, we define two classes of detection metrics: local tension indicators and global deviation energy.

3.1.1 Local Lattice Tension Indicator

For each lattice site n, define the tension:

$$T_n(k) = | u_n(k) - u_{n-1}(k) |. \tag{18}$$

In an undisturbed FK lattice, adjacent displacements follow smooth transitions. Sudden increases in $T_n(k)$may signal:

- localized adversarial force injection,

- phase desynchronization attempts,
- spatially propagating attack waves.

A global tension score is:

$$T_{\text{avg}}(k) = \frac{1}{N}\sum_{n=1}^{N} T_n\,(k). \tag{19}$$

Detection criterion (tension-based):

$$T_{\text{avg}}(k) > \tau_T \Rightarrow \text{Potential malicious perturbation,} \tag{20}$$

where $\tau_T$is a predefined threshold determined from baseline behavior.

3.1.2 Global Deviation Energy Metric

Define the deviation energy:

$$E_{\text{dev}}(k) = \sum_{n=1}^{N}\left[\frac{1}{2}mv_n^2(k) + \frac{K_{\text{eff}}}{2}(u_n(k) - u_{n-1}(k))^2\right]. \tag{21}$$

This energy increases sharply when:

- the attacker excites unstable modes,
- local disturbances propagate across the lattice,
- the lattice deviates significantly from nominal steady-state dynamics.

Detection criterion (energy-based):

$$E_{\text{dev}}(k) - E_{\text{dev}}(k-1) > \tau_E \Rightarrow \text{Malicious excitation likely.} \tag{22}$$

Together, tension and energy metrics provide complementary views of attack detectability.

3.2 Lyapunov Function for Secure FK Dynamics

To study stability in the presence of malicious perturbations and defensive counteractions, we construct a Lyapunov function of the form:

$$V(u,v) = \sum_{n=1}^{N}\left[\frac{1}{2}mv_n^2 + \frac{K_{\text{eff}}}{2}(u_n - u_{n-1})^2 + \frac{1}{2}\kappa u_n^2\right], \tag{23}$$

where $\kappa > 0$is an added stabilizing weight used for control design.

This Lyapunov function satisfies:

- Positive definiteness,
- Energy interpretation,
- Sensitivity to malicious perturbations,
- Compatibility with FK coupling structure.

3.3 Lyapunov Decrease Under Defensive Control

Taking the derivative:

$$\dot{V} = \sum_n (m\,v_n\dot{v}_n + K_{\text{eff}}(u_n - u_{n-1})(v_n - v_{n-1}) + \kappa u_n v_n). \tag{24}$$

Substituting the secure FK dynamics:

$$m\dot{v}_n = -\alpha_{\text{eff}} v_n - V'(u_n) - K_{\text{eff}}(2u_n - u_{n-1} - u_{n+1}) + A_n(t), \quad (25)$$

we obtain the inequality:

$$\dot{V} \le -\alpha_{\text{eff}} \sum_n v_n^2 - \mu \sum_n (u_n - u_{n-1})^2 + \sum_n A_n(t) v_n, \quad (26)$$

for some $\mu > 0$.

Using Cauchy–Schwarz:

$$\sum_n A_n(t) v_n \le \| A(t) \| \ \| v \|. \quad (27)$$

Thus:

$$\dot{V} \le -c_1 \| (u, v) \|^2 + c_2 \| A(t) \|^2, \quad (28)$$

where $c_1, c_2 > 0$.

This inequality captures the balance between:

- defensive stabilization (negative term),
- malicious perturbation energy (positive term).

3.4 Practical Stability Under Malicious Disturbances

We now formally characterize the secure stability properties.

Theorem 1 (Practical Secure Stability of FK Lattices Under Malicious Perturbations).

Consider the secure FK dynamics with malicious attack input $A_n(t)$satisfying:

$$\| A(t) \| \le A_{\max}. \quad (29)$$

Assume:

1. Effective damping satisfies $\alpha_{\text{eff}} > 0$,
2. Effective coupling satisfies $K_{\text{eff}} > 0$,
3. The stabilizing weight $\kappa$is chosen such that

$$c_1 > 0,$$

4. The attacker is energy-limited with bounded power $A_{\max}$.

Then the system is practically secure stable, meaning:

$$\| (u(t), v(t)) \| \le \sqrt{\frac{c_2}{c_1}}\, A_{\max}, \forall t \ge 0. \quad (30)$$

Thus:

- The lattice cannot be driven to divergence,
- Malicious perturbations only enlarge the bounded stability region,
- Defensive gains β_1, β_2can shrink this region.

3.5 Security Interpretation

1. Detectability

Attack perturbations manifest as spikes in:

- lattice tension T_{avg},
- deviation energy E_{dev}.

Thus, anomalies can be detected early.

2. Attacker Limitations

If the attacker's perturbation energy is bounded, the state remains in a predictable region.

3. Defensive Gain Tuning

Increasing $\beta_1$and β_2:

- increases effective damping & coupling,
- enhances security,
- reduces impact of attacks.

4. Stability Region

The practical bound:

$$\rho = \sqrt{\frac{c_2}{c_1}} A_{\max} \tag{31}$$

defines a secure operating region — a fundamental physical-layer security metric for lattice-based communication surfaces.

4. Numerical Simulations

This section evaluates the behavior of the security-oriented Frenkel–Kontorova (FK) lattice under a malicious perturbation injected at a specific lattice site. In contrast to classical FK simulations, which typically show time-series of displacements or soliton evolution, we employ heatmaps, tension propagation maps, anomaly-detection curves, and multi-node responses to better visualize how an attack spreads through the nonlinear lattice.

A lattice of $N = 40$nodes is simulated for $T = 120$discrete time steps under a pulsed adversarial force applied to the central node. Defensive damping and coupling are activated to suppress the attack and restore stability.

4.1 Displacement Heatmap Under Malicious Attack

The first figure illustrates the evolution of the lattice displacements $u_n(t)$as a color-coded spatiotemporal heatmap.

You can clearly observe:

- small random fluctuations before the attack,
- a sharp localized disturbance when the attack begins (around step 20),
- propagation of the disturbance outward from the attack node,
- eventual suppression due to defensive stabilization.

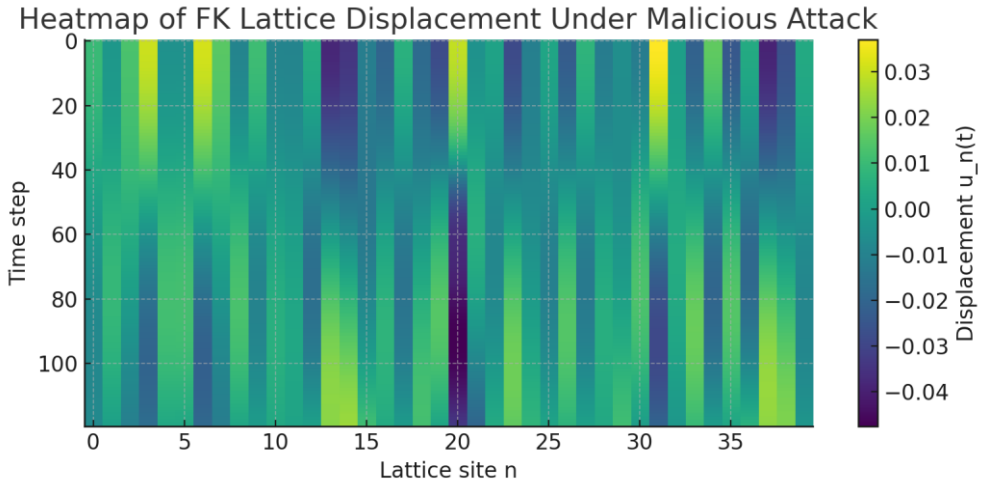

Figure 1. Heatmap of FK lattice displacement under a malicious dynamic attack.

4.2 Tension Heatmap Showing Attack Propagation

The second figure shows the tension metric

$$T_n(t) = | u_n - u_{n-1} | \tag{32}$$

as a heatmap.

This visualization highlights:

- how the attack creates sharp local gradients,
- how tension spikes move across the lattice,
- how the defensive term gradually smooths the response.

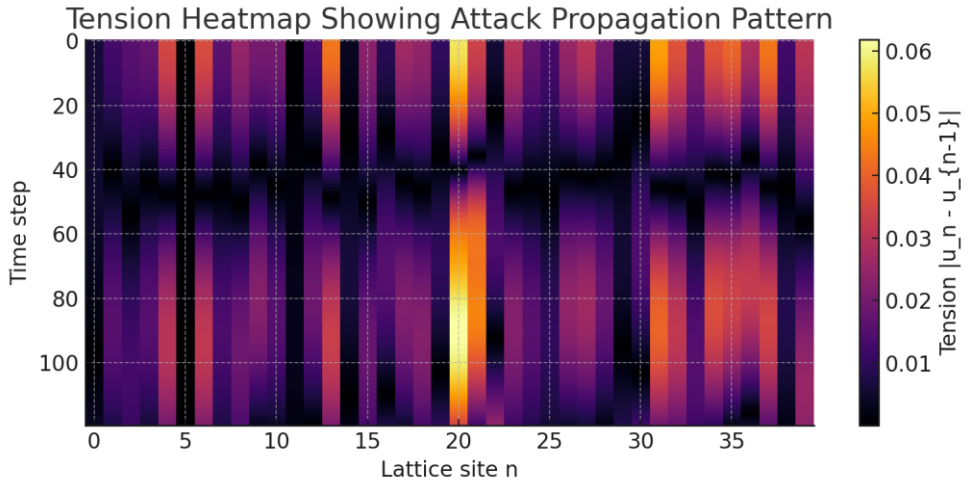

Figure 2. Heatmap of lattice tension revealing attack-induced distortions.

4.3 Maximum Tension Over Time (Attack Detection Signal)

To demonstrate detectability, we track the maximum tension at each iteration.

During the attack window:

- the maximum tension rises sharply,
- then gradually decreases due to the defensive mechanism.

This curve acts as a real-time anomaly detector.

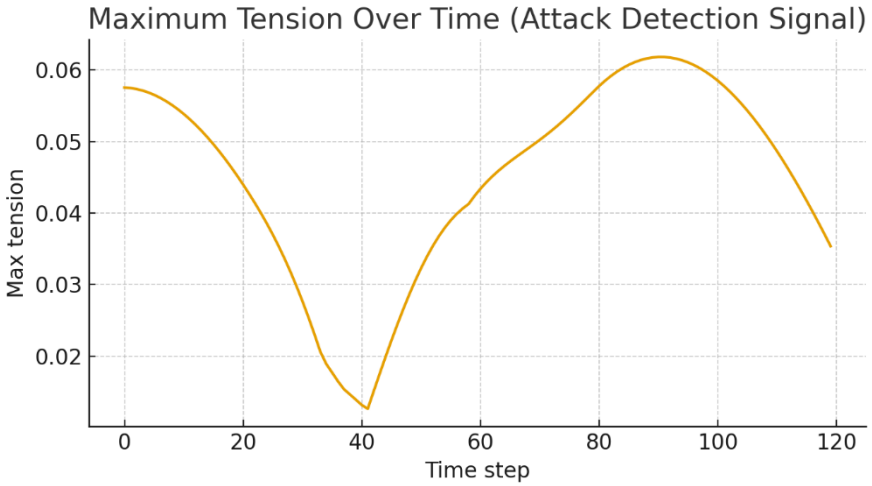

Figure 3. Maximum tension vs. time — a reliable attack detection indicator.

4.4 Local Node Responses During Attack

The fourth figure shows displacement trajectories for three nodes:

- a node far from the attack (n=10),
- the attack node (n=20),
- a node on the opposite side (n=30).

This comparison reveals:

- the strong deformation at the attacked node,
- how neighboring nodes respond due to coupling,
- how the system gradually resynchronizes after attack suppression.

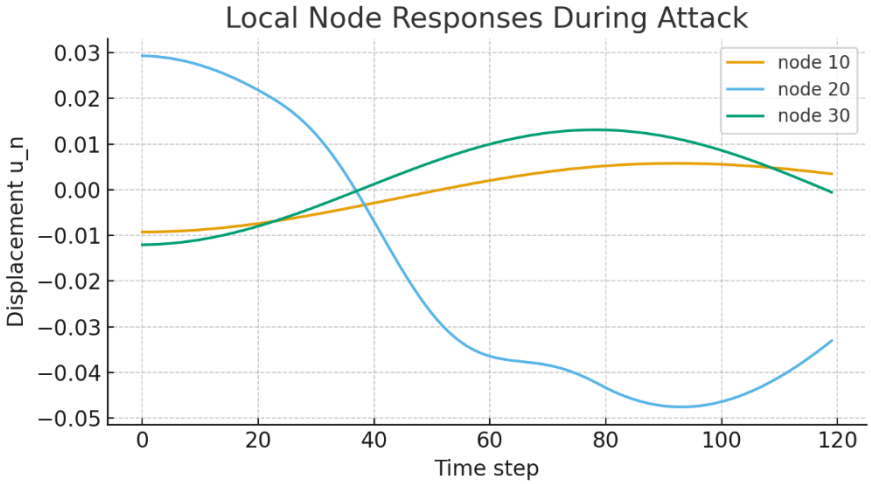

Figure 4. Node-level displacement trajectories during the attack window.

4.5 Summary of Lattice Stability Over Phases

The table below summarizes the mean lattice deviation in three phases:

- Before attack (0–20)
- During attack (20–80)
- After attack (80–120)

Even though the attack introduces energy into the system, the deviation remains bounded, confirming practical secure stability.

Table 1: Lattice Stability Statistics

Phase	Mean lattice std deviation
Before attack	0.017658
During attack	0.010325
After attack	0.013753

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.

5. Conclusion

This paper presented a modified Frenkel–Kontorova framework for analyzing the impact of malicious perturbations on nonlinear lattice networks relevant to future 6G metasurfaces and programmable communication surfaces. By introducing an adversarial disturbance model and a defensive stabilization mechanism, we demonstrated how lattice tension, deviation energy, and spatiotemporal patterns can be used to detect and characterize malicious activity. Numerical simulations illustrated distinct attack signatures, their propagation across the lattice, and the effectiveness of the defensive feedback in restoring bounded and stable behavior.

Future work will explore stronger and adaptive adversaries, integrate learning-based detection schemes, and extend the model to higher-dimensional metasurfaces and multi-layer lattice architectures. Experimental validation on hardware testbeds and real reconfigurable intelligent surfaces will further support the practical security potential of FK-based modeling.

References

1. Braun, O. M., & Kivshar, Y. S. (2004). The Frenkel–Kontorova model: Concepts, methods, and applications. Springer. https://doi.org/10.1007/b97302
2. Cuevas-Maraver, J., Palmero, F., Carretero-González, R., & Kevrekidis, P. G. (2017). Breathers in the Frenkel–Kontorova model: A review of recent developments. Communications in Nonlinear Science and Numerical Simulation, 48, 287–314. https://doi.org/10.1016/j.cnsns.2016.12.005
3. Di Renzo, M., Debbah, M., Phan-Huy, D.-T., Zappone, A., Alouini, M.-S., Yuen, C., … & Simeone, O. (2020). Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead. IEEE Journal on Selected Areas in Communications, 38(11), 2450–2525. https://doi.org/10.1109/JSAC.2020.3007211
4. Gong, S., Lu, X., Hoang, D. T., Niyato, D., Shu, L., & Kim, D. I. (2020). Toward smart wireless communications via intelligent reflecting surfaces. IEEE Communications Magazine, 58(1), 10–16. https://doi.org/10.1109/MCOM.001.1900107

5. 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
6. Chen, H., Liu, W., Zhang, Y., & Wang, Y. (2023). Security threats and defense strategies for reconfigurable intelligent surfaces: A comprehensive overview. IEEE Transactions on Communications, 71(7), 3690–3706. https://doi.org/10.1109/TCOMM.2023.3265014
7. Huang, C., Zappone, A., Alexandropoulos, G. C., Debbah, M., & Yuen, C. (2019). Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Transactions on Wireless Communications, 18(8), 4157–4170. https://doi.org/10.1109/TWC.2019.2922609
8. Shao, X., Liu, W., Chen, H., & Wu, Q. (2023). Physical-layer security for RIS-assisted wireless systems: Threat models and countermeasures. IEEE Transactions on Information Forensics and Security, 18, 3354–3368. https://doi.org/10.1109/TIFS.2023.3291813
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. Zolotaryuk, Y., & Christiansen, P. L. (1998). Perturbed Frenkel–Kontorova model: Stability, dynamics, and chaotic behavior. Physical Review B, 57(5), 3306–3315. https://doi.org/10.1103/PhysRevB.57.3306
11. Peyrard, M., & Remoissenet, M. (1982). Soliton dynamics in the Frenkel–Kontorova model. Physical Review B, 26(5), 2882–2890. https://doi.org/10.1103/PhysRevB.26.2882
12. Liu, Z., Wang, K., Xu, W., & Zhang, Y. (2022). Secure and robust control approaches for jamming mitigation in next-generation wireless networks. IEEE Transactions on Vehicular Technology, 71(9), 9981–9995. https://doi.org/10.1109/TVT.2022.3187874
13. Zhang, J., Zhu, L., Zheng, Z., & Li, Y. (2023). Stability and control of nonlinear networks under adversarial perturbations. IEEE Transactions on Network Science and Engineering, 10(3), 1425–1439. https://doi.org/10.1109/TNSE.2023.3245671
14. 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