Secure Time-Modulated Intelligent Reflecting Surface via Generative Flow Networks

Zhihao Tao, Athina Petropulu

Rutgers University - New Brunswick

Supported by ARO grant W911NF2320103 and NSF grant ECCS-2320568

Outline

1. Introduction
2. System Model
3. GFlowNet-Based TM-IRS Parameter Design
4. Results
5. Conclusion

Outline

1. Introduction
2. System Model
3. GFlowNet-Based TM-IRS Parameter Design
4. Results
5. Conclusion

Background

- **Wireless Security Challenge:** The broadcast nature of wireless propagation exposes information to unauthorized receivers.
- **Physical Layer Security (PLS):** Utilizes characteristics of the wireless medium (e.g., fading, noise, spatial diversity) to secure transmission, complementing or replacing cryptographic methods.
- **Directional Modulation (DM):** Embeds data into the spatial domain—legitimate receivers observe undistorted constellations, while eavesdroppers see scrambled signals[1].
- Compared to secrecy-rate optimization or artificial noise injection, DM offers **cost-effective and energy-efficient** secure transmission[2].

[1] Tao et al. 2024.
[2] Su et al. 2022.

Time-Modulated IRS

- **Time-Modulated Arrays (TMA):** Uses single-RF-chain with high-speed switches to periodically activate/deactivate antennas, generating harmonic-based scrambling in OFDM systems[3].
- TMA enables DM without multiple RF chains or channel knowledge but suffers from **power loss due to deactivated elements.**
- **Intelligent Reflecting Surface (IRS):** Passive metasurface with programmable phase shifts for beamforming[4].
- **Time-Modulated IRS (TM-IRS):** Introduces time modulation to IRS elements to achieve 3D directional modulation and compensate for TMA power loss[5].

[3] Ding et al. 2019.
[4] Yurduseven et al. 2020.
[5] Xu and Petropulu 2024.

Research Gap and Our Contribution

- **Limitations of Prior TM-IRS Designs:**
  - Rely on rule-based, closed-form TM-IRS parameter selection that guarantees undistorted reception in one direction only.
  - Do not scale to **multi-user scenarios.**

- **Our Approach:**
  - Not rule-based, supports multiple users, provides diverse, high-performing TM-IRS configurations.
  - Formulate TM-IRS parameter selection as a **deterministic Markov Decision Process (MDP)**.
  - Employ a **Generative Flow Network (GFlowNet)**[6] to learn a stochastic policy that samples TM-IRS parameter sets with probability proportional to their sum-rate reward.

[6] Bengio et al. 2023.

Outline

1 Introduction

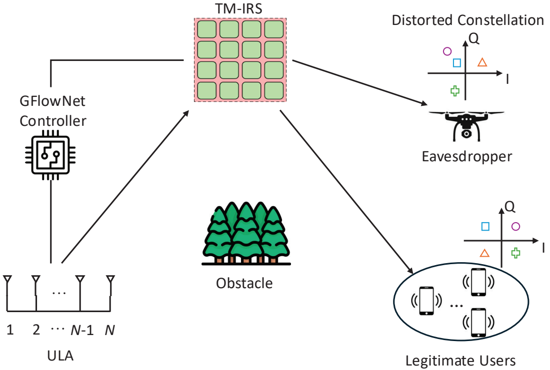
2 System Model

3 GFlowNet-Based TM-IRS Parameter Design

4 Results

5 Conclusion

System Setup



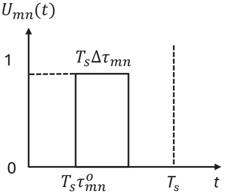
- **TM-IRS**: $M_x \times M_z$ reflecting elements, each controlled by a high-speed switch $U_{mn}(t)$ and a programmable phase shifter c_{mn}.
- **Assumptions:** (i) the transmitter knows the location of the legitimate user, but does not know the location of the eavesdropper; (ii) the channels of both the legitimate user and the eavesdropper are assumed to be known.

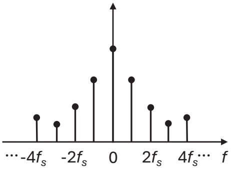
Time Modulation at the IRS

- OFDM Transmit Signal with K subcarriers:

$$e(t) = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} d(k) e^{j2\pi(f_c + k f_s)t}, \quad 0 \leq t < T_s$$

- Each IRS element periodically switches between "on" and "off" states by a periodic function $U_{mn}(t)$:





- Express via Fourier series — generating harmonics at multiples of subcarrier spacing f_s:

$$U_{mn}(t) = \sum_{l=-\infty}^{\infty} e^{j2\pi l f_s t} \Delta\tau_{mn} \, \text{sinc}(l\pi\Delta\tau_{mn}) e^{-jl\pi(2\tau^o_{mn} + \Delta\tau_{mn})}$$

Time Modulation at the IRS

- Define the far-field array factor of the (m, n)-th IRS element as

$$a_{mn}(\theta, \phi) = e^{-j\pi(m \sin\theta \cos\phi + n \sin\theta \sin\phi)}$$

- The received signal on subcarrier i, at direction (θ, ϕ) after demodulation:

$$y_i(\theta, \phi) = \sqrt{N/K} \sum_{k=0}^{K-1} d(k) V(i-k, \Omega_{mn}, \theta, \phi) + z_i$$

- The mixing coefficients (scrambling factor) are:

$$V(l, \Omega_{mn}, \theta, \phi) = \sum_{m=0}^{M_x-1} \sum_{n=0}^{M_z-1} a_{mn}(\theta_T, \phi_T) c_{mn} a_{mn}(\theta, \phi) \times \Delta\tau_{mn} \mathrm{sinc}(l\pi\Delta\tau_{mn}) e^{-jl\pi(2\tau_{mn}^o + \Delta\tau_{mn})},$$

where $\Omega_{mn} = \{c_{mn}, \Delta\tau_{mn}, \tau_{mn}^o\}$ represents the TM-IRS parameter configuration.

Optimization Objective

- $V_j \triangleq V(j, \Omega_{mn}, \theta_c, \phi_c)$ for $j \neq 0$ can be treated as interference.
- For u-th user (U legitimate users in total) at (θ_c, ϕ_c), SINR and achievable sum-rate can be defined as:

$$\mathsf{SINR}_i = \frac{\eta |V_0|^2}{\eta \sum_{j \neq 0} |V_j|^2 + \sigma^2}, \quad \eta = N/K$$

$$C_{\mathsf{total}} = \sum_{u=1}^{U} \sum_{i=0}^{K-1} \log_2(1 + \mathsf{SINR}_i)$$

Optimization objective: maximize the total achievable sum rate while imposing a phase constraint for each legitimate user

$$\max_{\Omega_{mn}} \; C_{\mathsf{total}} \qquad \text{s.t. } |\arg(V_0)_u| \leq \xi_u, \; \forall u$$

Outline

1. Introduction
2. System Model
3. GFlowNet-Based TM-IRS Parameter Design
4. Results
5. Conclusion

Overview of the Proposed Method

- **Optimization challenge:**
  - Nonlinear and nonconvex optimization
  - Intractability of closed-form solutions

- **Idea:** Discretize TM-IRS parameters $\Rightarrow$ Formulate TM-IRS parameter selection as a deterministic Markov Decision Process (MDP) problem $\Rightarrow$ Leverage a **flow-based GenAI** method to sample high-reward configurations efficiently.

- **GFlowNet:**
  - Uses the **flow-matching principle** to ensure consistency between forward and backward transitions.
  - Samples configurations **proportionally to their reward (effective sum rate)**.
  - Learns a **stochastic policy** that generates diverse high-quality solutions instead of a single optimum.

MDP Formulation

- Each IRS element (m, n) has three parameters:

$$\Omega_{mn} = \{c_{mn}, \tau_{mn}^{o}, \Delta\tau_{mn}\}$$

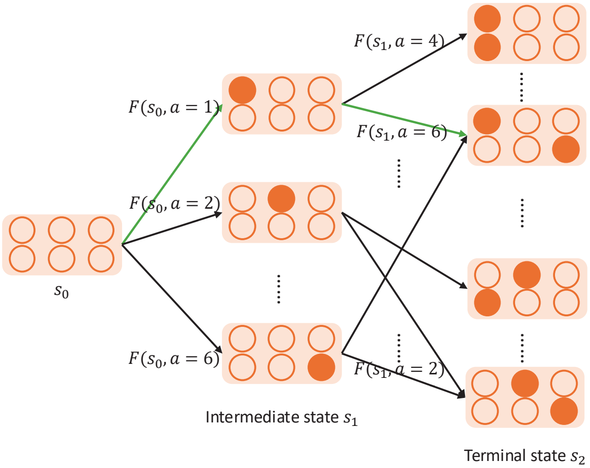
$$\angle c_{mn} \in [0, 2\pi),\ \tau_{mn}^{o}, \Delta\tau_{mn} \in [0, 1)$$

- Discretization:

$$\begin{aligned} c_{mn} &\in \{e^{j0}, e^{j2\pi/Q_1}, \ldots, e^{j2\pi(Q_1-1)/Q_1}\}, \\ \tau_{mn}^{o} &\in \{0, 1/Q_2, \ldots, (Q_2-1)/Q_2\}, \\ \Delta\tau_{mn} &\in \{0, 1/Q_3, \ldots, (Q_3-1)/Q_3\}. \end{aligned}$$

- Flow matching: $F_{\text{in}} = R + F_{\text{out}}$
  An example of the GFlowNet-based TM-IRS parameter selection, where two parameters are optimized, each with three discrete values.

MDP Formulation



Intermediate State: partial assignment of TM-IRS parameters; **Action:** choosing one value for an unassigned parameter; **Terminal state:** complete configuration of all IRS parameters; **Trajectory**: a sequence of actions from the root (initial) state to a terminal state.

Learning via GFlowNet

- **Objective:** Learn a stochastic policy that samples TM-IRS configurations Ω with probability proportional to their reward $R(\Omega)$.
- **Reward–Effective sum rate:**

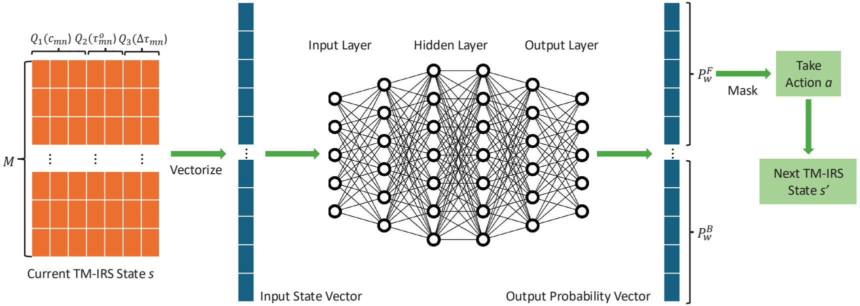
$$R = C_{\text{total}} \prod_{u=1}^{U} H(\xi_u - |\arg(V_0)_u|)$$

  where $H(\cdot)$ is the Heaviside function enforcing phase constraints and ξ_u is is a modulation-specific threshold.
- **Training:**
  - GFlowNet models forward/backward flows using neural networks.
  - Trained with the *Trajectory Balance (TB) loss:*

$$L_{TB}(\tau) = \left(\ln \frac{Z_w \prod_t P_F(s_t|s_{t-1})}{R(x) \prod_t P_B(s_{t-1}|s_t)} \right)^2$$

- After training offline, the GFlowNet is deployed online to sample high-reward Ω.

Learning via GFlowNet



An illustration of the GFlowNet-based TM-IRS design framework.

Outline

1. Introduction
2. System Model
3. GFlowNet-Based TM-IRS Parameter Design
4. Results
5. Conclusion

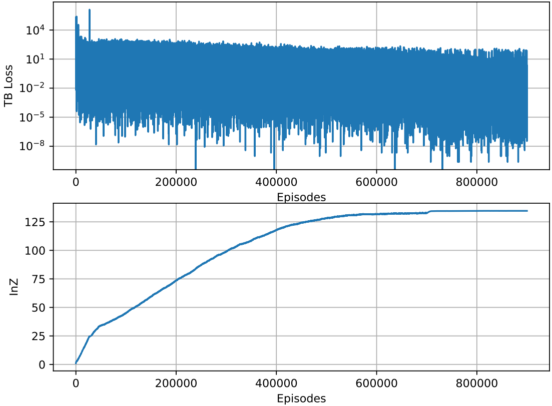
Simulation Setup

- System parameters:
  - IRS with $M_x = M_z = 6$ reflecting elements; ULA transmitter with $N = 8$ antennas.
  - $K = 16$ OFDM subcarriers; QPSK modulation.
  - SNR = 0 dB; path loss normalized to 1 for simplicity.

- Discretization: $Q_1 = 16$, $Q_2 = Q_3 = 8$
- GFlowNet architecture:
  - Feedforward neural network with three hidden layers (256 neurons each).
  - Trained offline on 9×10^5 trajectories using an Apple M3 Max chip (36 GB RAM); learning rate $10^{-2} \to 10^{-3}$.

- Symbol error rate (SER) is adopted as the performance metric.

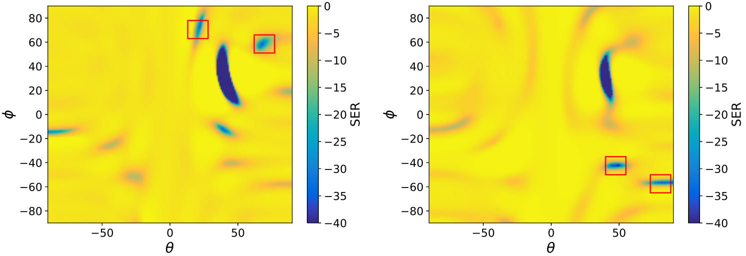
Training Performance



- TB loss **monotonically decreases**, indicating flow-balance convergence.
- Partition function $\ln Z$ stabilizes after $\sim 8 \times 10^5$ episodes.
- Despite $\sim 10^{65}$ possible configurations, convergence achieved with $< 0.000001\%$ of the search space.

Single-User Directional Modulation

- Legitimate user located at $(\theta_c, \phi_c) = (40^\circ, 30^\circ)$.
- **Comparison:** Rule-based vs. proposed GFlowNet-based design.
- Both methods achieve low SER in the desired direction.

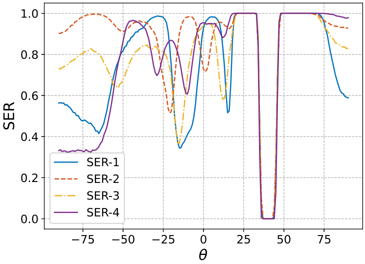


(a) (b)

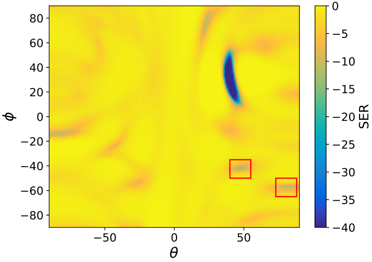
Spatial SER maps: (a) rule-based; (b) GFlowNet-based.

Enhancing Security via Pattern Diversity

- GFlowNet naturally generates multiple high-reward TM-IRS configurations.
- Switching among them introduces **time-varying TM-IRS patterns**, increasing privacy.
- (a) Four sampled configurations applied sequentially (256 symbols each); (b) averaged SER map shows reduced leakage in undesired directions.



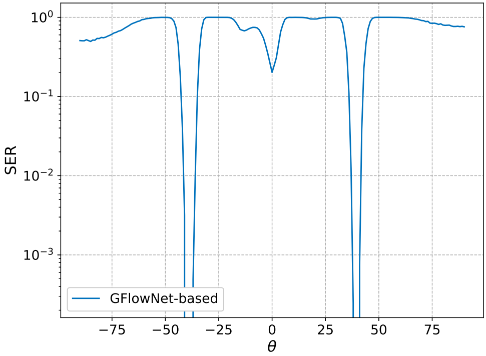
(a)



(b)

Multi-User Scenario

- Two legitimate users: $(40°, 30°)$ and $(-40°, 30°)$.
- Constraint: $|\arg(V_0)_u| \leq \pi/5$ for both users.
- GFlowNet jointly optimizes TM and IRS phase parameters for both directions.
- Achieves low SER in both legitimate directions while maintaining high SER elsewhere.



Outline

1. Introduction
2. System Model
3. GFlowNet-Based TM-IRS Parameter Design
4. Results
5. Conclusion

Conclusion

- Conventional rule-based TM-IRS designs are restricted to single-user secure transmission.
- We have proposed a GFlowNet-based generative framework for TM-IRS parameter optimization, modeling the discretized parameter selection process as a deterministic MDP with learned stochastic policies.
- The proposed method efficiently generates diverse, high-reward TM-IRS configurations, achieving low SER for legitimate users and strong scrambling in other directions.
- It enables scalable and AI-driven secure TM-IRS design, with promising extensions to integrated sensing and communication (ISAC) systems.

Thank You!

Questions are welcome.

Email: zt118@scarletmail.rutgers.edu

- Bengio, Yoshua et al. (2023). “Gflownet foundations”. In: *Journal of Machine Learning Research* 24.210, pp. 1–55.
- Ding, Yuan et al. (Aug. 2019). “Time-Modulated OFDM Directional Modulation Transmitters”. In: *IEEE Trans. Veh. Tech.* 68.8, pp. 8249–8253.
- Su, Nanchi et al. (2022). “Secure dual-functional radar-communication transmission: Exploiting interference for resilience against target eavesdropping”. In: *IEEE Trans. on Wireless Communications* 21.9, pp. 7238–7252.
- Tao, Zhihao, Zhaoyi Xu, and Athina Petropulu (2024). “How Secure Is the Time-Modulated Array-Enabled OFDM Directional Modulation?” In: *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*. Seoul, Korea.

Xu, Zhaoyi and Athina Petropulu (2024). “Time-Modulated Intelligent Reflecting Surface for Waveform Security”. In: *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*. Seoul, Korea, pp. 8986–8990. DOI: 10.1109/ICASSP48485.2024.10447621.

Yurduseven, Okan, Stylianos D Assimonis, and Michail Matthaiou (2020). “Intelligent reflecting surfaces with spatial modulation: An electromagnetic perspective”. In: *IEEE Open Journal of the Communications Society* 1, pp. 1256–1266.