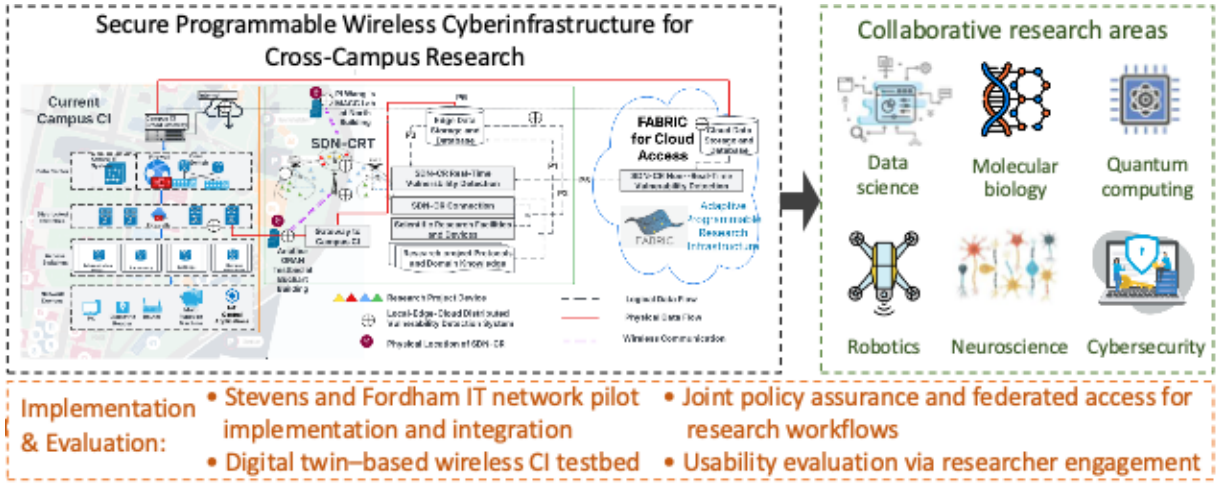
WRAP: Programmable Wireless Infrastructure with Formal Assurance for Cross-Campus Research

PI: Ying Wang (Stevens Institute of Technology) Co-PI: Juntao Chen (Fordham University)



Collaboration and Usability Challenge Addressed

- Collaborative research requires dynamic cross-campus wireless access, but the state of practice security approaches limit flexibility.
- WRAP combines open program infrastructure with formal assurance to align usability and compliance. Researcher-facing tools simplify configuration while IT teams maintain visibility and control.

Technical Cybersecurity Solution

- Formal assurance translates researcher goals into verifiable policies.
- Runtime anomaly detection ensures continuous, secure operation.
- Replicable architecture unites programmability, assurance, and usability.

Benefits to Scientific Cyberinfrastructure

- Enables secure, policy-compliant collaboration across campuses.
- Reduces friction between researcher agility and IT enforcement.
- Supports diverse workflows in genomics, AI, robotics, quantum, and more.
- Provides reusable open-source toolkits and training materials for adoption.

Risks Versus Potential For Advances

- **Risk**: Unforeseen domain regulations, cross-campus policy conflicts, and stakeholder priorities may limit seamless adoption.
- **Payoff**: Cross-domain researcher and IT engagement builds a replicable, evolving architecture with error resilience, sustainability, and scalability beyond campuses.

Result Dissemination Plans

- Open-source release of WRAP toolkits, policy models, and verification datasets.
- Deployment templates, dashboards, and training materials for replication at peer institutions.
- Publications, workshops, and cross-campus demos to engage both researchers and IT teams.

Programmatic Details

- 3 year project started on September, 2025
- Led by Stevens Institute of Technology and with Fordham University

This material is based upon work supported by the National Science Foundation under Grant No. 2530916

WRAP: Programmable Wireless Infrastructure with Formal Assurance for Cross-Campus Research
WRAP – Dataset Needs and Sharing Plan

PI: Ying Wang (Stevens Institute of Technology) Co-PI: Juntao Chen (Fordham University)

Generated Data

- Formal-guided fuzz testing results (misconfiguration detection, attack traces).
- WRAP testbed datasets (slice definitions, runtime anomalies, protocol deviations).
- Usability metrics from researcher interactions (configuration success rates, alert responses).

Collaboration and Usability Challenge Addressed

- Code: MIT License
- **(open-source on GitHub: wrap-ci/wrap-platform)**
- Datasets: CC BY-NC License;.

Formats & Metadata

- Structured in CSV, JSON, YAML for interoperability.
- Metadata aligned with Dublin Core / IEEE standards for discoverability.

Reusability

- Formal verification, network anomaly detection, and policy compliance benchmarking.
- Supports integration with OSDF/NDP initiatives

This material is based upon work supported by the National Science Foundation under Grant No. 2530916