Y9.ET1.2: Secure System-Level Invariant Derivation and Validation

Project Leader: Jonathan Kimball

Faculty: Bruce McMillin

Students: Bokang Zhou

1. Project Goals

This project extends the results achieved in year 8 and focuses on expanding the scope of invariants. The primary focus has been developing a dynamic invariant. For a given nonlinear system (e.g., a FREEDM system), a set of small-signal models may be derived, corresponding to a set of steady-state operating points, corresponding to a set of cyber commands. Conditions may be derived that guarantee stability as the system switches between these different operating points. The method uses Lyapunov functions for each mode and timing restrictions.

2. Role in Support of Strategic Plan

This work is a crucial link between physical system analysis and the operation of the DGI. The specific details are unique to FREEDM. However, it also demonstrates general principles and a framework applicable to other cyber-physical systems. The use of invariants for security furthers the field of cyber-physical security.

3. Fundamental Research, Technological Barriers and Methodologies

The proposed approach uses level sets of the various Lyapunov functions. For each steady-state operating point, a small ellipsoid forms a level set that is the target. A larger ellipsoid encloses the smaller ellipsoids of the other operating points. The time required to transition from the larger ellipsoid to the smaller ellipsoid is the minimum dwell time that guarantees stability.

4. Achievements

The invariant approach has been previously demonstrated as a guard against incorrect actions by various DGI nodes. Specifically, the voltage invariant can block power transfers that will cause voltage collapse and the line flow invariant can block power transfers that would overload any line. The new dynamic invariant will extend this to a succession of power transfers, not just a single transfer, that collectively would cause instability.

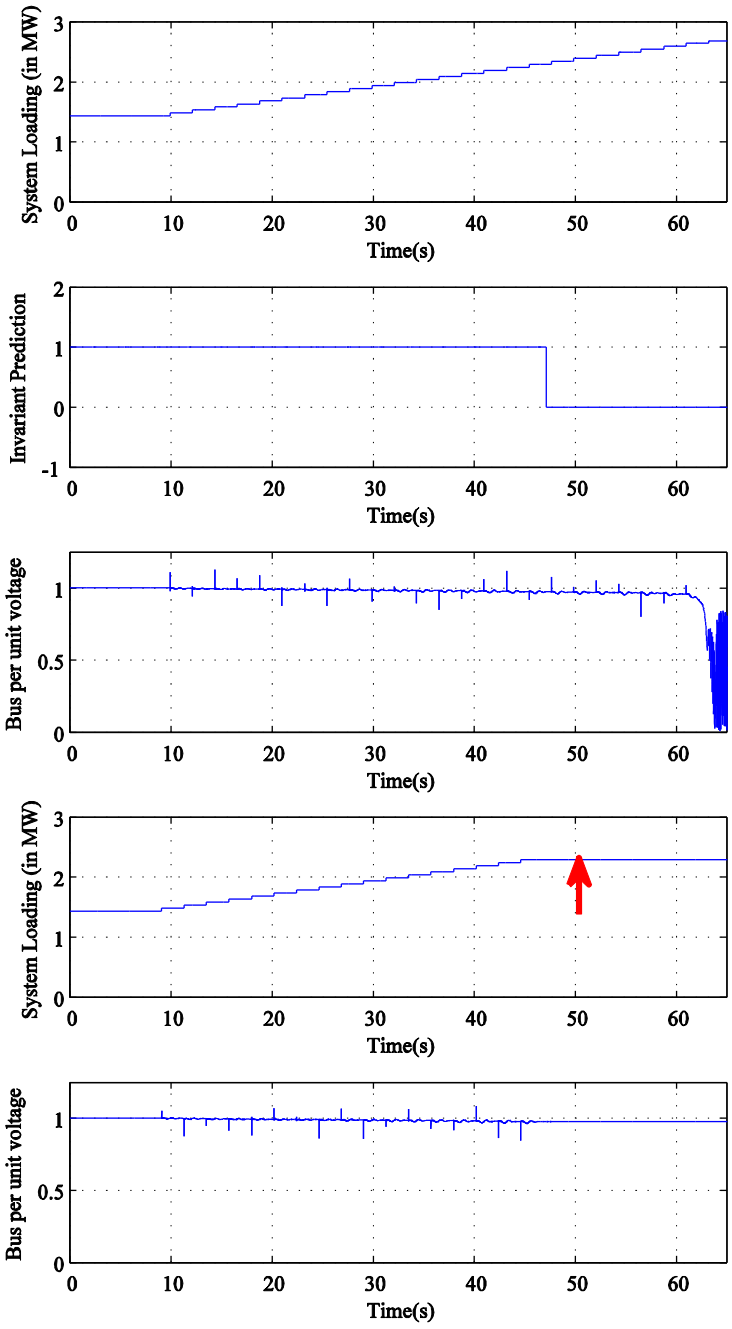

Figure 1: Example operation of voltage stability invariant. The top three graphs indicate load, the invariant truth value, and the bus voltage. In this case, the invariant is evaluated but not used, and the voltage collapses. In the bottom two graphs, the invariant truth value is used to guard against an incorrect transaction, and the bus voltage remains stable.

5. Other Relevant Work Being Conducted Within and Outside of the ERC

This project is related to an affiliated project that was funded by NSF this year, a collaborative project led by Kimball and also including McMillin and Chow: “Collaborative Research: Breakthrough: Secure Algorithms for Cyber-Physical Systems.” In the affiliated work, the invariants are being integrated with Chow’s reputation algorithm.

6. Milestones and Deliverables

Q1 (3/31/2017) – Proposed dynamic invariant validated in Simulink
Q2 (6/30/2017) – Dynamic invariant integrated on HIL and validated
Deliverable for SV (04/2017): Demonstrated dynamic invariant.
Final Deliverable (08/2017): Secure and Resilient FREEDM system through secure application integration

7. Plans for Next Five Years

In addition to the dynamic invariant, multiple invariants are being integrated with real algorithms developed on a distributed computing platform. This is expected to extend beyond the FREEDM system to include other cyber-physical systems.

8. Member Company Benefits

9. References