

Automatic Failure Recovery for Software-Defined Networks

Maciej Kuźniar*, Peter Perešíni*, Nedeljko Vasić (EPFL),
Marco Canini (TU Berlin / T-Labs), and Dejan Kostić (IMDEA Networks)
http://prophet.networks.imdea.org/
*These authors contributed equally to this work

Network failure recovery

Link and switch failures happen



All SDN controllers need to implement failure recovery logic

- Not all controllers need complex recovery
- Mixed application logic and recovery logic makes controllers difficult to maintain and reason about
 - high risk of errors

Goals

Decouple failure recovery and controller logic

Provide controller independent failure recovery

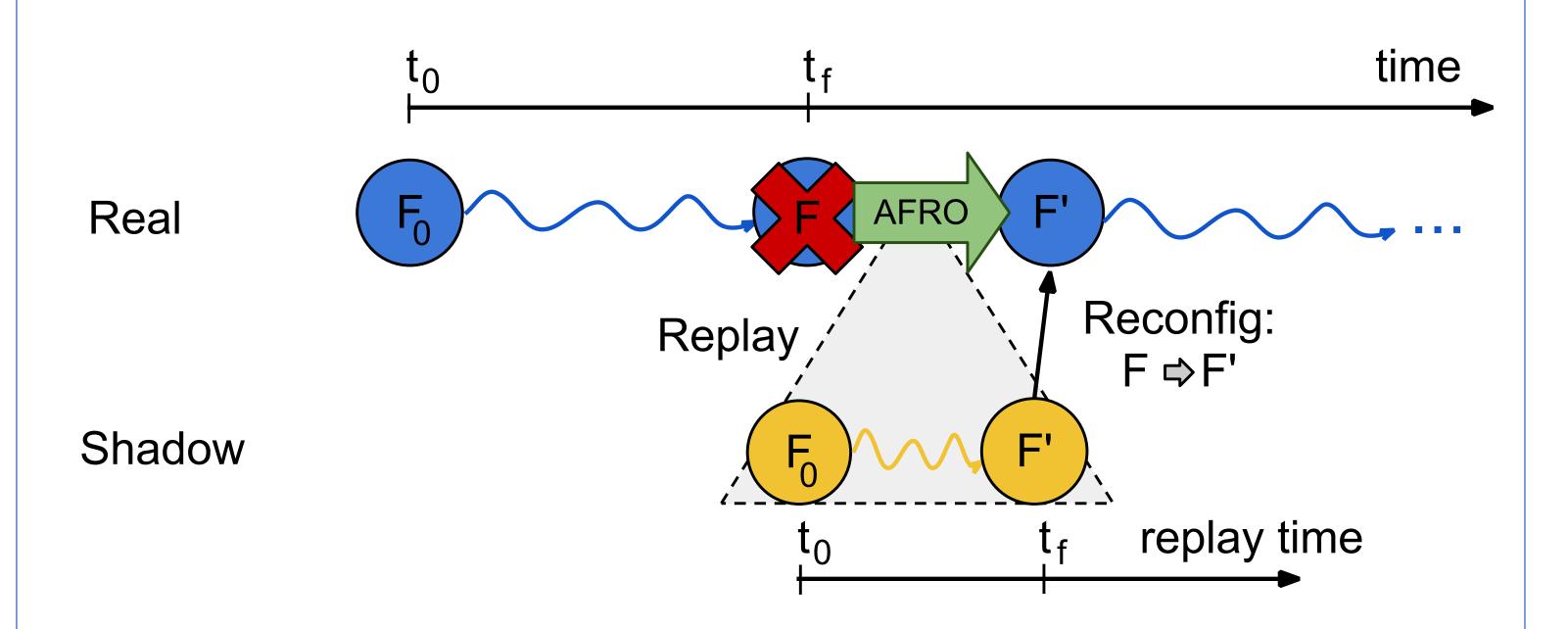
But also:

- Help planning maintenance
- Simplify fast prototyping
- Provide ground truth for failure recovery
- Assist in analyzing "What if" scenarios

Approach: Record and replay

Insight: instead of reacting to failure, start a new controller that works on a network without the failed element.

This way we provide the controller with an abstraction of static network



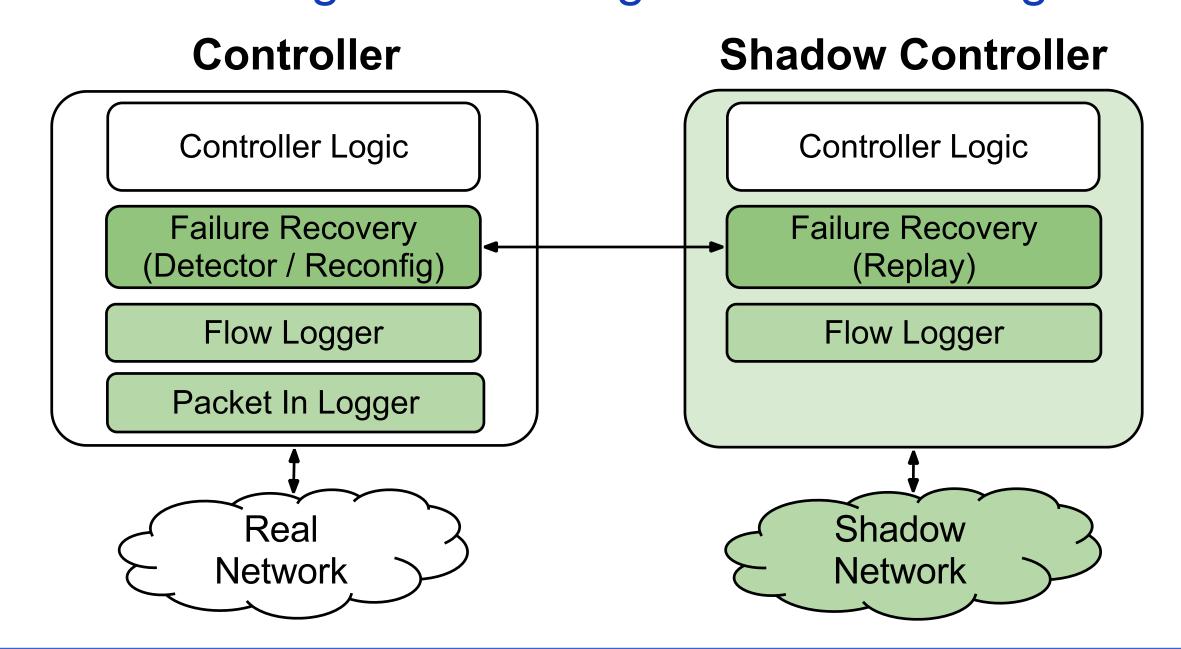
Record inputs to the controller

After failure:

- 1. Create an emulated network without the failed component
- 2. Start a fresh controller in the emulator
- 3. Replay events in the emulator
- 4. Compute the difference between real network state and emulated state
- 5. Update the real network to match the emulation

Architecture

Requires no changes in the original controller logic



Assumptions

AFRO requires controller to satisfy following requirements:

- Controller works correctly on a static network
- Controller is event driven
- Controller is deterministic

Challenges

Replay needs to be quick and efficient

Replay needs to resemble real execution

Network update and controller switch needs to be efficient

Replay optimizations

Pruning PacketIn events – replay only necessary events

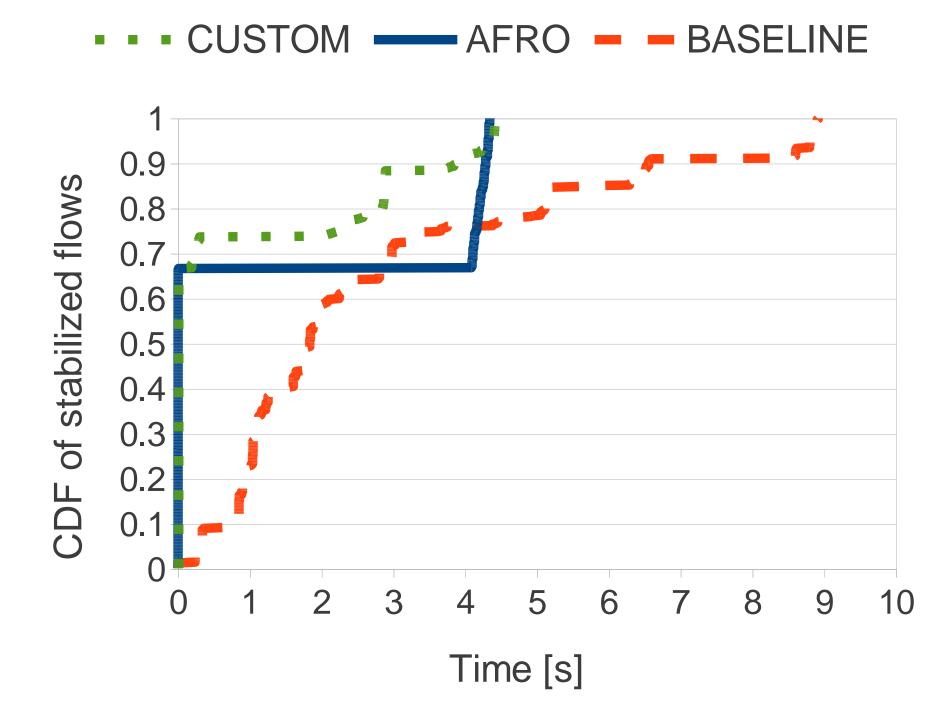
- Replay edge
- Replay edge causing FlowMod
- Replay edge with dependencies

Parallel replay

- Independent events can be replayed in parallel
- Force order of dependent events

Evaluation

- Experiments with a real network testbed
- AFRO has no impact on flows unaffected by the failure



Recovery time with AFRO is comparable with custom controller specific failure recovery solution

