UNIVERSITY OF TWENTE.

UNIVERSITY OF AMSTERDAM

Increasing the Transparency, Accountability and Controllability of multi-domain networks with the UPIN framework

Rodrigo Bazo, Leonardo Boldrini, Cristian Hesselman, Paola Grosso

Introduction

Introduction

- Demands for a more trustworthy Internet are constantly increasing
- Emerging critical service providers are one of the main drivers behind such demand
- Although a success, the current Internet infrastructure lacks essential capacities
  - E.g. users cannot control nor verify their data paths
- Goal: Define needed components and functions to achieve transparency, accountability and controllability in Inter-domain networks.

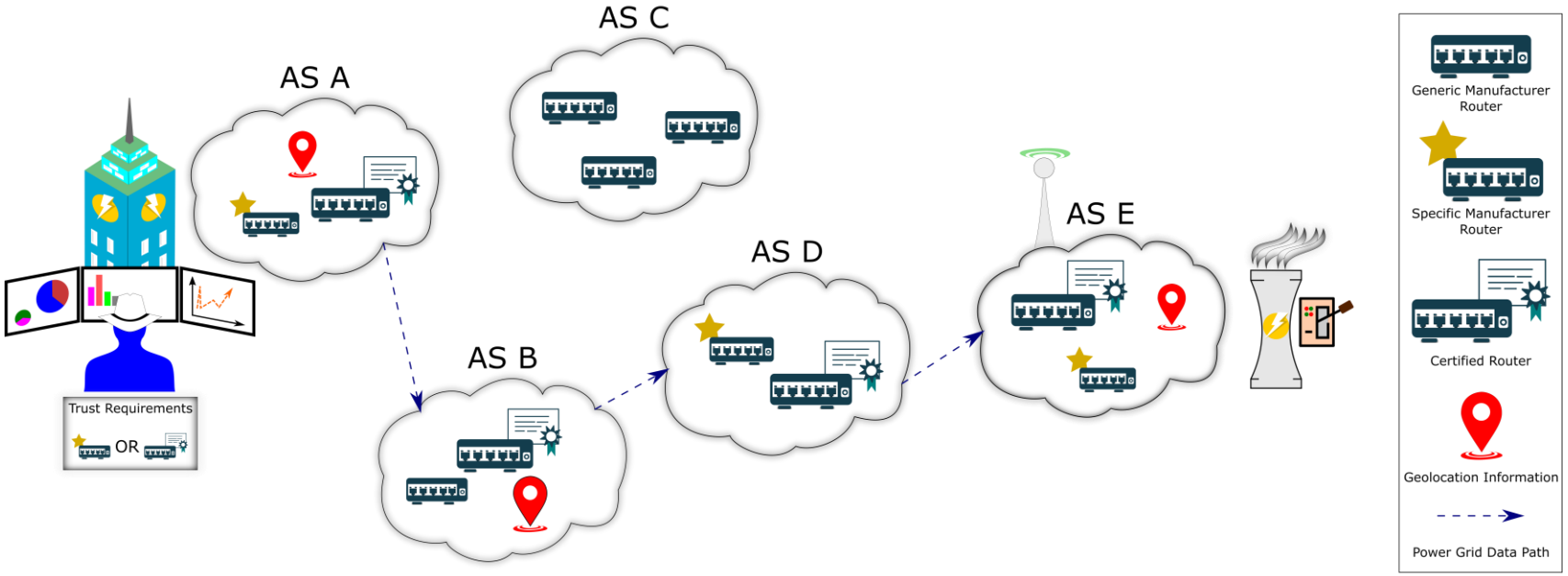
New Internet Security Requirements

New Internet Security Requirements

- Future Internet applications require higher levels of trust from the Internet
  - Cyber-physical and critical applications services have direct impact in people's lifes

- We analyze the requirements based on three essential pillars:
  - Transparency: Capability of a network to provide information about its infrastructure
  - Accountability: Capability of a network to describe the way it processes data
  - Controllability: Capability of a network to allow their users to specify how the network (or chains of networks) must handle their data

Smart Grid Example



New Internet Security Requirements

- Involved parties will require more transparency and accountability from networks
  - Particularly in multi-domain scenarios (e.g. Internet)

- Involved parties require more control over how the network transports their data

Existing Tech

Existing Technologies

- There are technologies there that partially solve our problem. But not as a whole.

Solution	Transparency	Accountability	Controllability
PDP	✓	✓	x
SR	x	x	✓
PAN	x	✓	✓

UPIN Framework

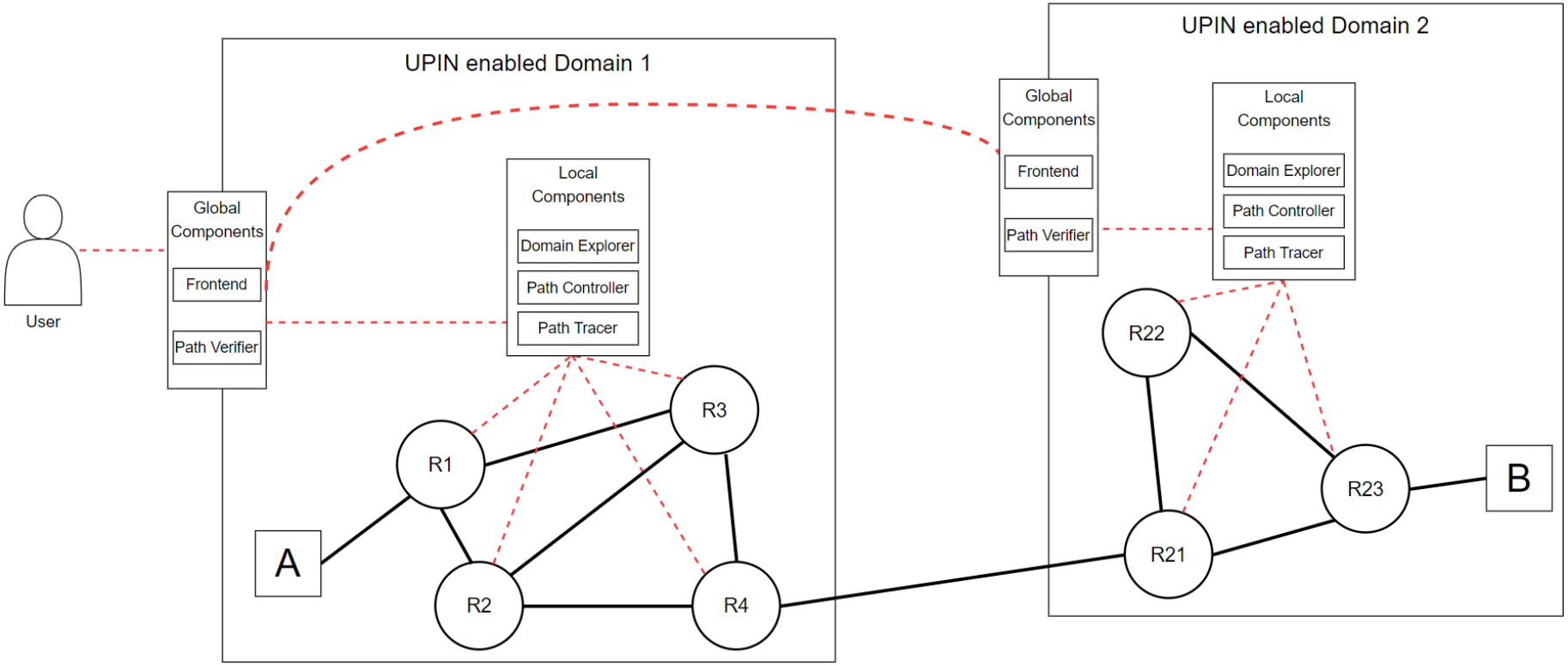
UPIN Framework

- The framework consists of a group of functions and components that, when coupled together, enable our requirements on Transparency, Accountability and Controllability to be fulfilled
- The UPIN framework does not mandate the underlying data plane technology
- UPIN stand for User-driven Path Verification and Control in Inter-domain networks

UPIN Framework Components

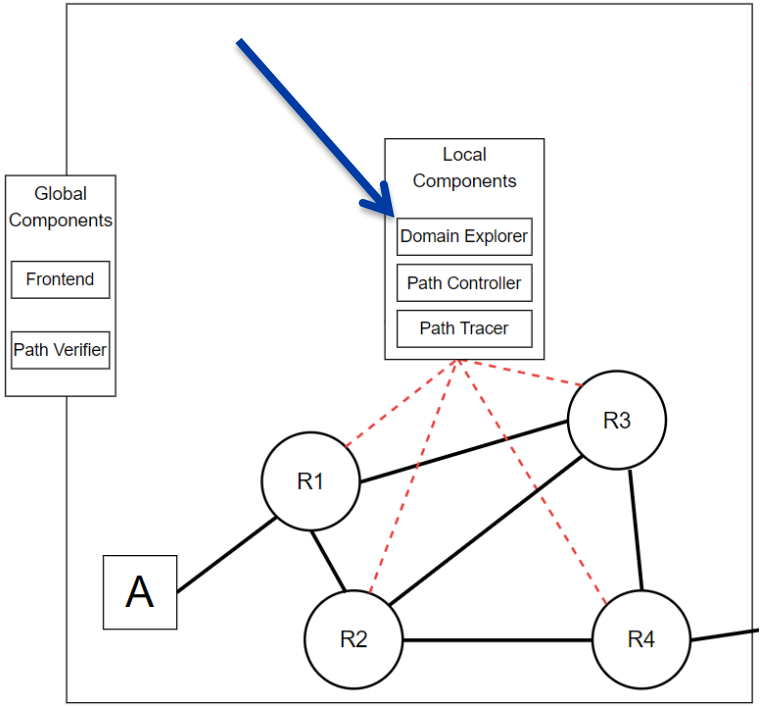
Component	Transparency	Accountability	Controllability
Domain Explorer	✓	✓	✓
Path Controller	*x*	*x*	✓
Path Tracer	✓	✓	*x*
Path Verifier	✓	✓	*x*
Frontend	✓	✓	✓

UPIN Framework



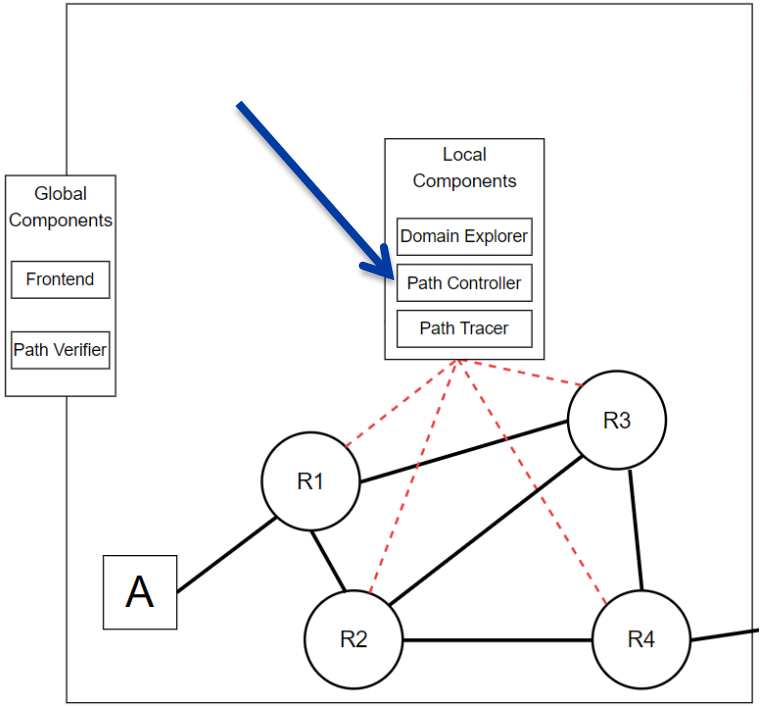
Domain Explorer

- Retrieves and stores metadata from it's domains equipment properties, e.g.:
  - Routers location
  - Routers source-code and firmware version
- Has a local scope only
- Provides up-to-date local information for other domains through the Frontend



Path Controller

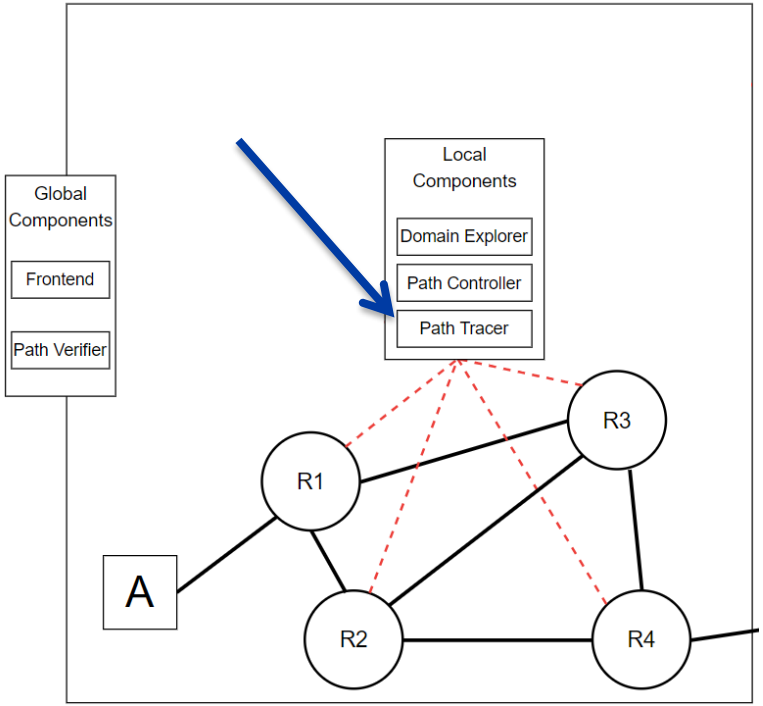
- Forwards user's data based on specified preferences
- Has local scope only



Path Tracer

- Gathers real-time measurements of data plane traffic and stores it for verification purposes

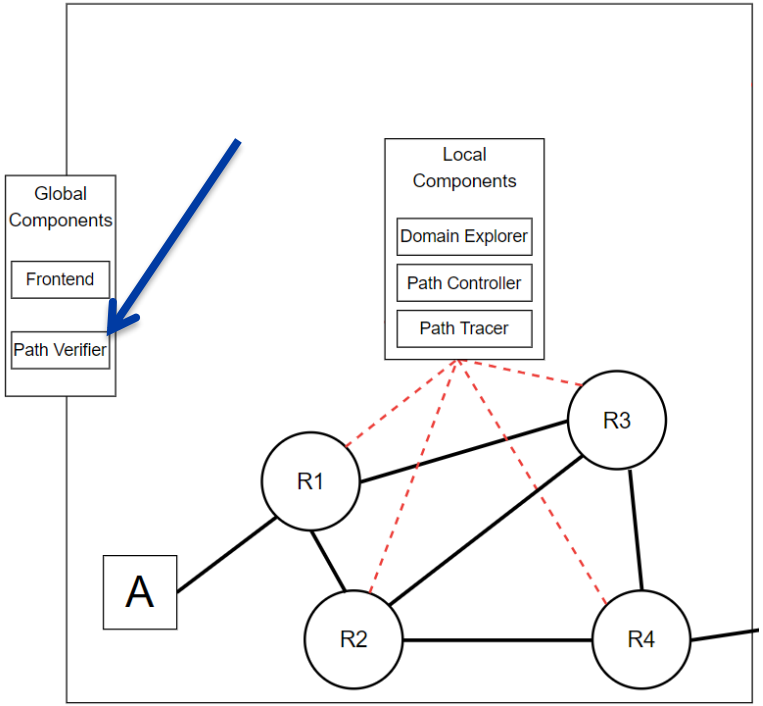
- Has local scope only



Path Verifier

- Checks if user's preferences are being respected
  - Either in real-time or a posteriori

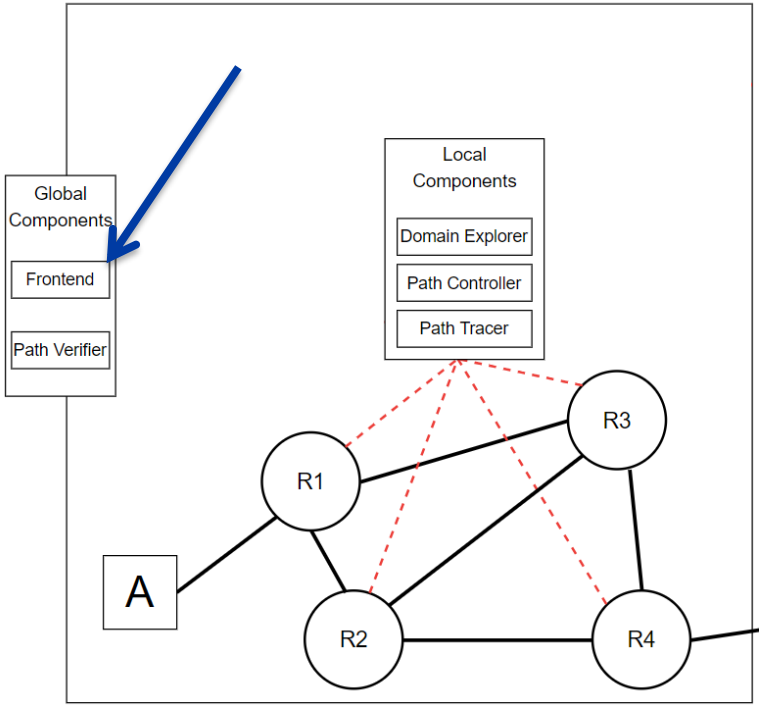
- Feedbacks information to other domains in order to enable end-to-end compliance check



Frontend

- Provides the interface for the user to set up his preferences

- Provides the interface for domains to exchange information



Initial Experiments

Initial Experiments

- Initial experiments focus on single-domain scenario and on the Path Controller component
- Using Segment Routing we enable users to steer their traffic through specific Virtual Network Functions (e.g. Firewall and Packet Mirror)
- In this experiments:
  - A traffic generator emulates the User
  - A SDN controller which gathers the network topology and deals with external instructions

Initial Experiments

- The main testbed for experimentation is the 2STiC testbed
  - Multi-domain star-shaped network of P4 programmable routers located in the Netherlands

- Path Verification experiments with P4 are also under development and will be deployed on the testbed

Final Remarks

Final Remarks

- The framework presented in this work focuses on assessing the lack of Transparency, Accountability and Controllability in Inter-domain networks, such as the Internet
- We observe that network operators must share meta-data about their infrastructure in order to achieve this
- Our presented architecture organizes required network functions and components that pave the road towards a Responsible Internet

Open Challenges

- Investigate how to disclose network infrastructure information (e.g. router attributes) without opening up potential security breaches
- Investigate incentives and benefits (e.g. financial or performance) of disclosing information and adopting the proposed solution
- Verification and attestation of information provided by other domains are a major point of interest as well

Thanks! Questions?

This research received funding from the Dutch Research Council (NWO)