

DIGITAL SOVEREIGNTY IN PRACTICE

ciena



UNIVERSITY OF AMSTERDAM

LEVERAGING INT AND ML FOR A RESPONSIBLE INTERNET

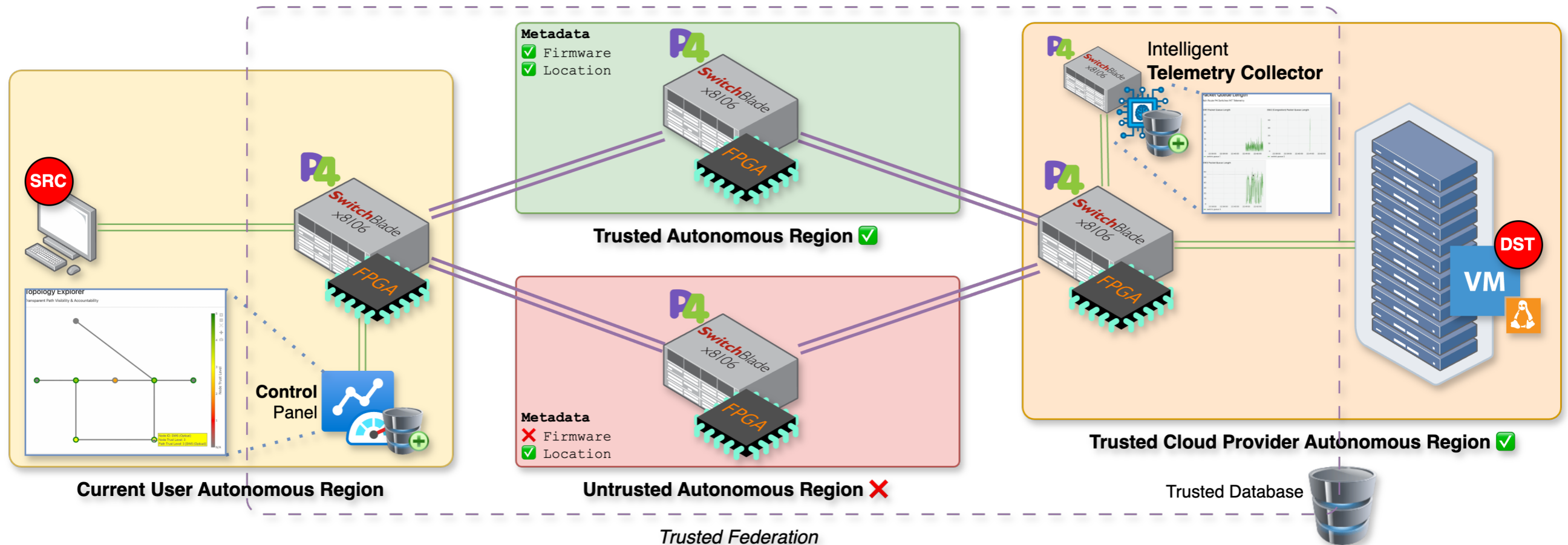
KEY POINTS OF RESPONSIBLE INTERNET

- ▶ **Digital Autonomy:** Ensuring society's critical systems are resilient against manipulation and surveillance.
- ▶ **User Empowerment:** Allowing individuals to choose trusted networking equipment and specify data handling preferences.
- ▶ **Transparency and Trust:** Enabling verification of good-faith operator actions and precise tracing of incidents or attacks.
- ▶ **Emerging Technologies:** Leveraging programmable networks, Machine Learning, and Intent-Based Networking to enhance security and control.
- ▶ **Real-time Visibility:** Programmable Data Planes and In-band Network Telemetry can provide detailed network insights directly within data packets.

CONTRIBUTION

- ▶ **User-defined Data Path Control:** Designed an operator platform that empowers users to specify, monitor, and verify their data flows using INT for transparency.
- ▶ **RL-based Route Optimization:** Developed a Reinforcement Learning approach within a programmable P4 switch that autonomously selects the optimal and secure network paths based on real-time INT metrics and user-defined preferences—directly in the data plane without control plane intervention.
- ▶ **Real-world Validation:** Demonstrated the practicality and feasibility of our Responsible Internet solution through realistic experimentation conducted on the FABRIC network infrastructure.

DEMONSTRATION SCENARIO



- ▶ 4 USA Sites, simulating 4 operators in 4 different states.
- ▶ 4 P4 FPGA switches that embed telemetry data.
- ▶ Intelligent telemetry collector choosing data flow based on user preferences.

SCENARIO I – USER INTENT-DRIVEN TRAFFIC CONTROL

- ▶ Users define personalized preferences (trusted devices, geographical locations) through the Control Panel.
- ▶ **Live Topology Visualization:** Real-time network topology network map displays the user data flow.
- ▶ **Dynamic Data Path Reconfiguration:** Users specify trust criteria, prompting the network P4-programmable switches to autonomously adapt data flow paths accordingly.
- ▶ **Real-time Integrity Monitoring:** Users actively monitor data flow integrity and compliance with trust settings directly through the Control Panel.

SCENARIO II – AUTONOMOUS LEARNING-DRIVEN IN-NETWORK CONTROL

- ▶ **INT-based Real-time Metrics:** Network devices continuously embed telemetry metadata into packets, capturing detailed performance and trust metrics.
- ▶ **Reinforcement Learning (RL) Integration:** An Intelligent Telemetry Collector uses RL algorithms within programmable devices to process telemetry data, determining optimal path based on user-defined trust policies. The RL-based agent autonomously learns and dynamically adjusts network paths, responding in real-time to changing security conditions and network states.
- ▶ **Transparent AI-driven Control:** Users can observe AI-driven route optimization decisions and resulting network adaptations transparently via the Control Panel.

PATH MONITORING

The screenshot shows a web browser window with the URL `localhost:1043/topo`. The page title is "ISP Portal" and the main heading is "Topology Explorer" with the subtitle "Transparent Path Visibility & Accountability".

Menu:

- Home
- Trust Flow Monitoring**
- Data Flow Preferences
- AI Training
- About

Topology Explorer:

The network diagram consists of five nodes and several connections. A central node is highlighted with a green tooltip:

- Node ID: Your Operator (FPGA SWID#1)
- Node Trust Level: 9
- Path Trust Level: 4 [Untrusted Autonomous Region (FPGA SWID#2)]
- Location: UCSD
- Device: Cisco

A vertical "Trust Level" legend on the right side of the diagram shows a color gradient from "None" (dark grey) to "Max" (dark green), with numerical markers from 1 to 9. The central node is colored dark green, corresponding to a trust level of 9.

UNIVERSITY OF AMSTERDAM

USER TRAFFIC FLOW PREFERENCES

ISP Portal - OFC25 UvA Demc x +

localhost:1043/control

ISP Portal

Menu

- Home
- Trust Flow Monitoring
- Data Flow Preferences**
- AI Training
- About

Data Flow Preferences

Set-up your preferences of how your data are handled in the Internet.

Your Preferences

Manual Configuration

AI selection based on your Trust Tolerance

Selected value: AI selection based on your Trust Tolerance

Your Location

San Francisco (ws-isp)

Report a problem | © OpenStreetMap contributors

Manually Exclude Regions

Your data will never enter the regions you exclude.

You have selected ['North Path (nt-isp)']

UNIVERSITY OF AMSTERDAM

POC EVALUATION

- ▶ **Real-time Path Tracing:** Embedding P4-switch metadata into packet headers using INT, eliminating the need for external probes or tracing software.
- ▶ **Dynamic User Control:** Real-time user-driven path customization based on specified trust preferences.
- ▶ **Adaptive Routing Validation:** User preference driven path selection.

ciena

DR. ANESTIS DALGKITSIS



UNIVERSITY OF AMSTERDAM

THANK YOU