

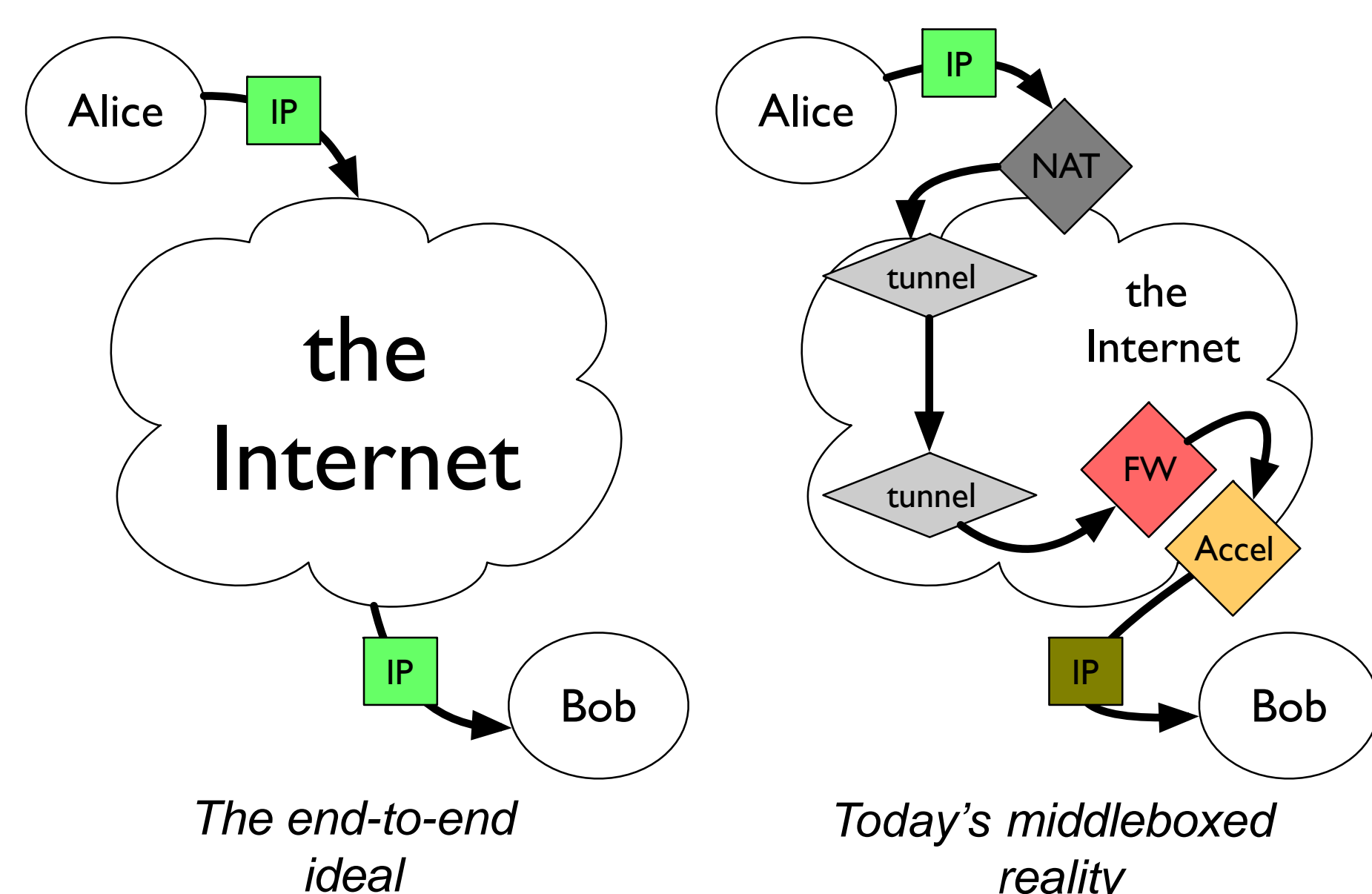
Measurement-based Protocol Design

Gorry Fairhurst (University of Aberdeen), Mirja Kühlewind (Networked Systems Group, ETH Zurich), and Diego Lopez (Telefonica I+D)

IN-NETWORK FUNCTIONS AND ENCRYPTION

Many **middleboxes** in current generation mobile networks [1]

- e.g. for NATs, firewall, or performance enhancing as transcoding often based on **clear text information** in protocol headers/payload
- e.g., TCP sequence and acknowledgement numbers to measure RTT for performances diagnostics



Three driving forces that presents a need for architectural changes:

Expanding deployment of encryption
to protect end-user privacy

Restoration of the
end-to-end principle
in the face of
increasing ossification

Dependency on
in-network functionality
to support
network operations

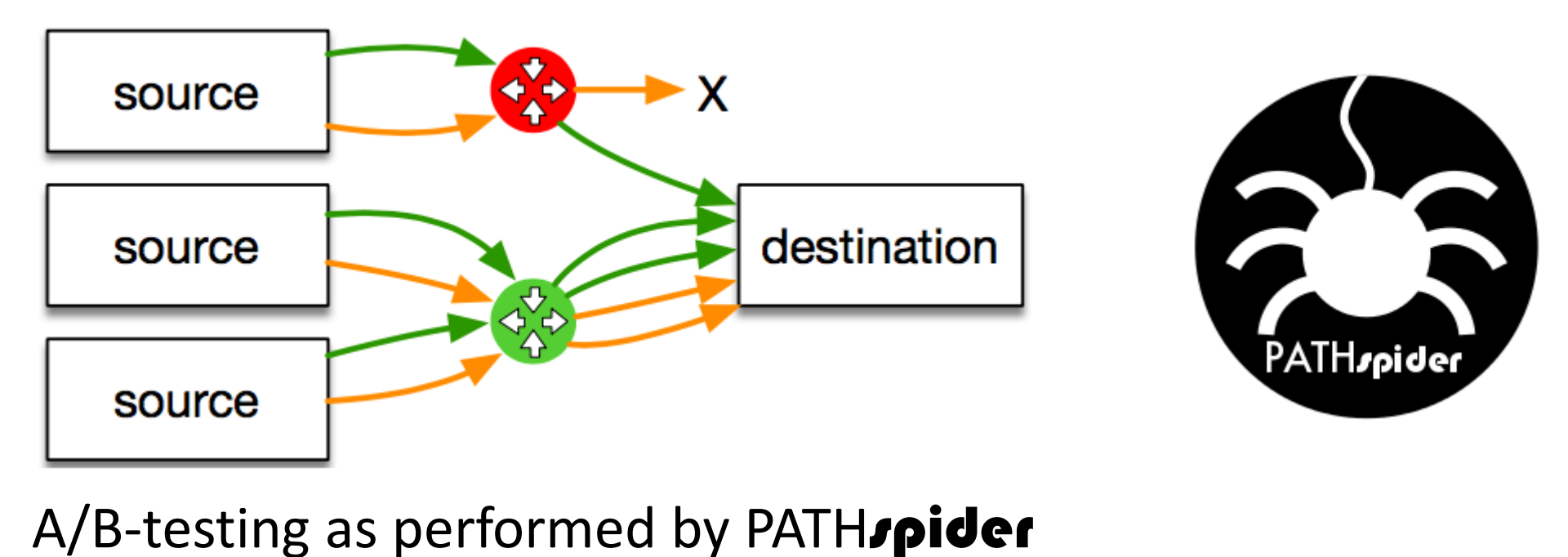
This raises new questions on the design of transport protocols:

- How does encryption impact existing deployed infrastructure?
- What options may exist to design new protocols with explicit support for certain in-network function?
- What form of operational support would need to be offered when these new protocols are deployed?

[1] Z. Wang, Z. Qian, Q. Xu, Z. M. Mao, and M. Zhang, "An untold story of middleboxes in cellular networks," in ACM SIGCOMM, 2011.

MEASUREMENT AS PART OF THE DESIGN PROCESS

- Using **PATHspider** to measure Internet path transparency, publicly available on GitHub <https://pathspider.net/>



- Experimental evaluation focusing on Mobile Broadband network, using MONROE nodes connected to up to 3 providers and WiFi: <https://www.monroe-project.eu/>

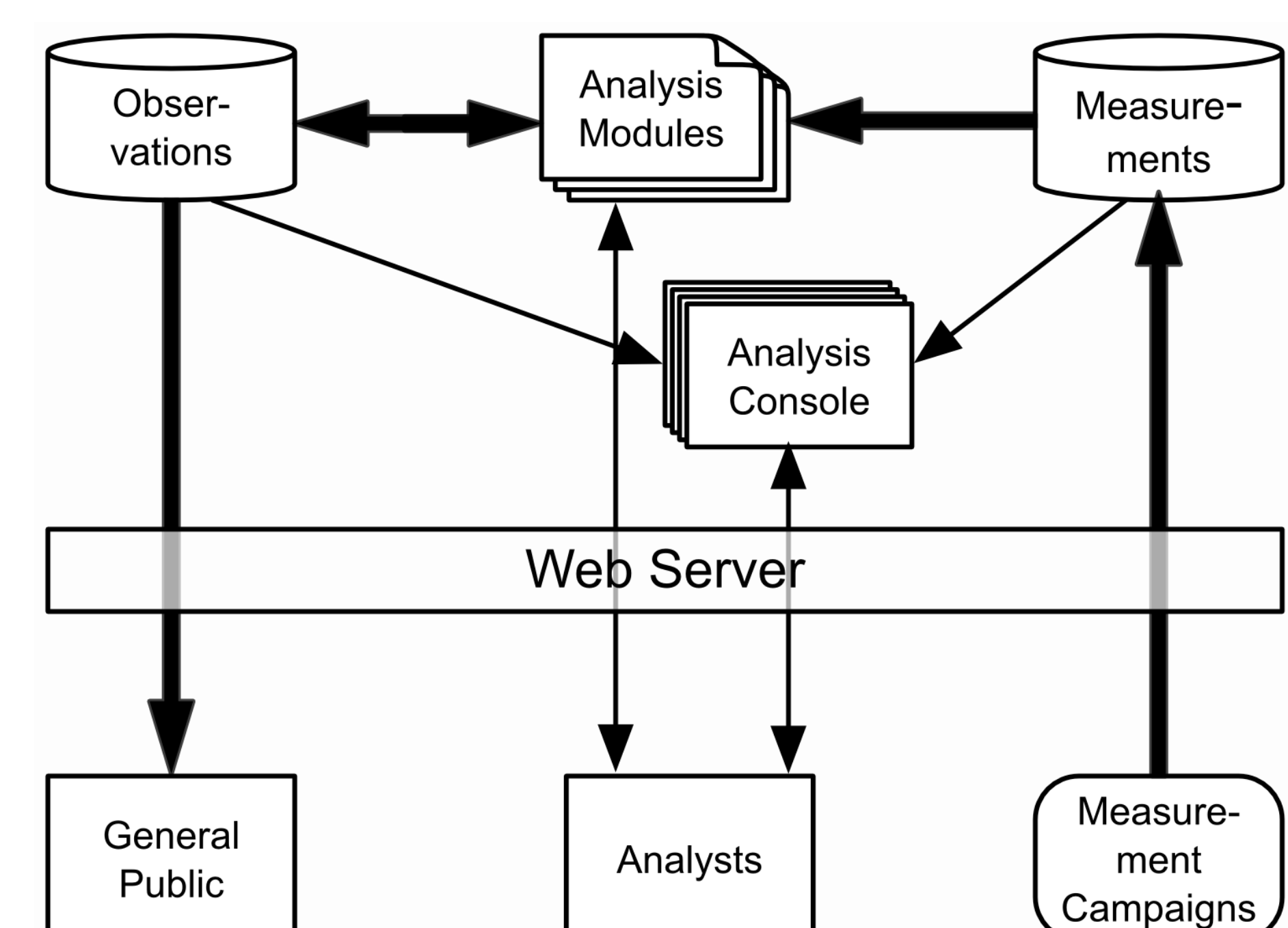


- Complemented measurement of the path with tools such as Tracebox: <http://www.tracebox.org/>

- Large-scale data collection from diverse sources in the Path Transparency Observatory (PTO): <http://observatory.mami-project.eu/>



- Observation:** a given *condition c* was observed on a given *path p* at a given *time t*
 - e.g. that ECN was successfully negotiated, or TFO works



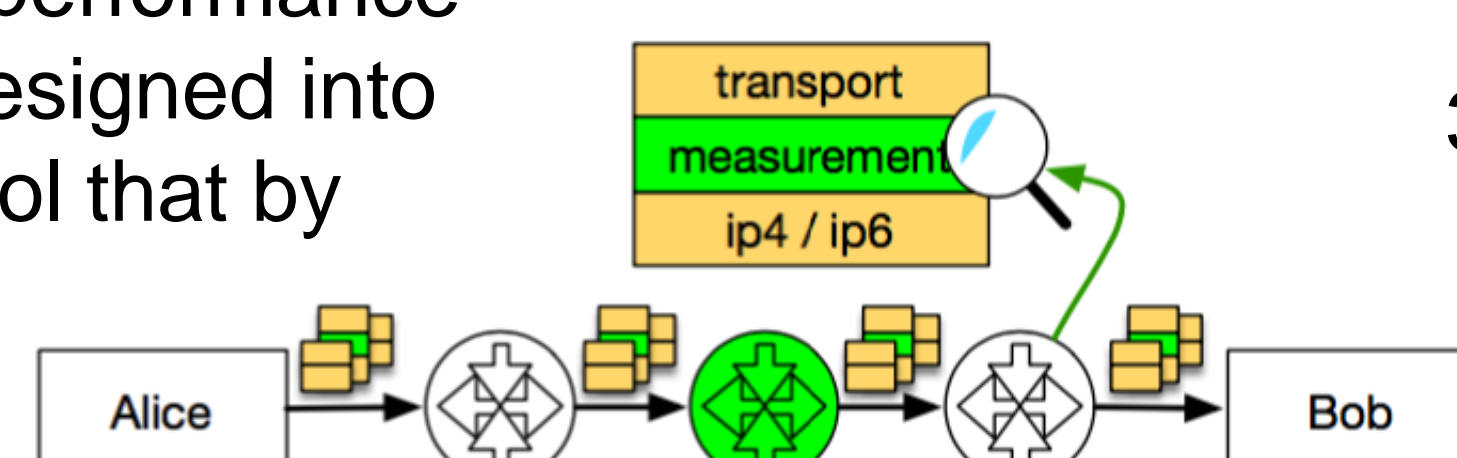
PROTOCOL DESIGN FOR MEASUREMENT

The availability of large scale measurement data enables a new approach to protocol design:

→ **Maps of middlebox manipulation** within the Internet provide background for design decisions about **protocol engineering and evolution**.

Goals

- Increase the likelihood that new protocols will be deployable across the entire Internet, regarding the range of effects from middlebox manipulation on various packet headers
- Build-in support for in-network performance measurement to be explicitly designed into next generation network protocol that by default encrypt all end-to-end protocol information



Design Principles

- Information exposure has to happen under explicit endpoint control
- Least exposure of minimum amount of information required by the proposed mechanism to solve the identified problem, in this case in-network measurement
- Trust by verify under the assumption that two endpoints have a trust relation for integrity protection and encryption but there is no requirement for an explicit trust relationship with the network

The *Path Layer UDP Substrate* (PLUS) proposes a framework for information exposure with a focus on measurements and diagnosability in a transport-protocol-independent way: see <https://datatracker.ietf.org/doc/draft-trammell-plus-spec/>