Optimized, automated and protective: Shaping the future of networks

Christian Jacquenet
christian.jacquenet@orange.com
I have a dream.

Networks help optimizing service quality and continuity in an always-on, digitally inclusive communication world

• Advanced forwarding schemes for robust and scalable multi-service, context- and power-aware, privacy-friendly networking

Network automation at large is a reality

• From dynamic service parameter exposure and negotiation to service fulfillment and assurance

Networks can detect and anticipate attacks way before they reach their targets

• Introducing protective networking, on the road to collaborative networking
Optimize.
The network becomes a digital assistant

Multi-path forwarding schemes

- Thanks to the evolution of transport protocols (MPTCP, QUIC)

The network establishes multi-path communications on behalf of the end-user

- Between multi-interfaced CPE/UE and Transport Converters (TC)
Workflow transport mode (e.g., unencrypted, encrypted, “leased line” service)

13th IFIP Wireless and Mobile Networking Conference, Oct. 21-22, 2021, Montreal, Canada
A (green) business opportunity.

Business path (selected)

Best hop-by-hop path

Unsuitable network (bad reputation, environmentally unfriendly, etc.)
Energy consumption matters.

Telcos to play a key role in achieving some of UN’s SDGs

• SDG#7 is one of them

Energy-aware networking

• Advertise consumed and available power
• Compress data
• Optimize signaling

IPv6 IoT networking paved the way

• Energy-inferred multi-metric dynamic route computation
Automate.
Seriously?
Welcome to the real world.

Lots of declarative tasks Vendor-agnostic framework remains a nice-to-have Automation remains embryonic
At last?
Acquire, learn and compute.

Input data

Computation logic

Output data
A bit of advice.

Think global but keep control, always.
  • Control loops and feedback mechanisms are instrumental for proper operation

Be open but preserve savoir-faire.
  • Standard protocols and data models keep vendor lock-in away
  • Open source should foster research, not hinder it

AI can help but demands extreme caution.
  • From intent interpretation to deterministic decision-making process
  • Service-inferred scalability and privacy preservation issues (to name a few)

Fill the gaps but be pragmatic.
  • No one-size-fits-all solution
Protect.
Detect, signal and mitigate.  

An anticipative attack mitigation framework

- Whatever the nature of the attack

Mitigation is performed as close to the source as possible.
And then some.

Assist, exchange and mitigate at a global scale.
Collaborate?
Towards automated multi-domain service production?

A three-step approach

1. Business owner identifies possible partners according to customer’s intent
2. Negotiation cycles are dynamically triggered
3. Business owner and partners then proceed with resource allocation assuming successful negotiation

Business Owner:
- Expresses intent towards Business Partners
- Accepts (declines) offers from Business Partners
- Makes an offer to customer
- Manages service orders

Customer:
- Expresses intent to Business Owner
- Orders service

Business Partner:
- Makes an offer to Business Owner(s)
- Allocates resources as contribution to the service
Truly end-to-end?
This is challenging.
This is even more challenging.

How to identify the most relevant partners?
How can a trust model be enforced, where all interested parties can safely collaborate to deliver the service (slice)?
What information needs to be exchanged between partners to deliver and operate the service (slice)?
What are the boundaries in terms of respective responsibility?
What guarantees can be provided?
Thank You!