Architectures and Incentives for Network and Application Collaboration

Jari Arkko

Senior Expert, Ericsson Research *

Member, IAB *

*) Affiliation and membership provided only for information. Opinions expressed here are author's opinions only.

Motivation – What Is My Interest?

- Long-time observer of the evolution and the ecosystem
- Have an interest in things that improve our digital lives
- I believe that network and applications collaborating is a good thing
  - Wanting a more collaborative Internet, maintain its distributed nature, and take care of security in the broadest sense

Very curious about

- Deployment incentives
- Successes and failures
- Alternatives
- Information sharing
- Security
- Communities

Scope

- Past practices
- Influential trends
- Current state

- Opportunities

- Design guidance
- Research challenges
- Related work

Past practices

Interaction and integration practices:

- Name- and address-based policies
- Protocol message analysis and modification
  - Often using implicit information, e.g., derived from in-clear end-to-end information such as transport protocols data that happened to be available
- Content or deep packet inspection-based policies
- Traffic flow analysis
- Interactions based on explicit agreements and signalling
- Purely business- and agreement-level arrangements
- No interaction

Examples

Goal: provide “good” service to a class of applications (e.g., streaming)

We could:

- look at addresses or names if they match known streaming services
- look at HTTP requests for type of media
- analyze interpacket-arrival times and traffic directionality
- signal the ISP that this flow is a streaming one
- buy a subscription that has enough bandwidth to support streaming

Downsides with packet analysis –based practices

- Basing behavior on information that may be incomplete / wrong
- Application may not know what triggers desired behaviour
- Ossification
- Systemic incentives against more secure protocols
- Creating an expectation that network elements can see rich data about flows

Influential Trends 1

Technical trends:

- Encryption of { data, headers, control protocols }
- Protocol, system, and ecosystem evolution to make the above easy
- Speed of change is increasing

- Limiting data collection even at primary servers - an emerging trend?

Influential Trends 2

Business trends:

- Migration of some functions to Internet-based services
- Consolidation and centralization of services
- Desire for most applications to ensure they are in control of the user’s end-to-end experience
- Growing networking needs for what are at any particular time the popular applications

Influential Trends 3

Societal trends:

- Increased reliance on IT
- Concern for the security of networks & IT systems
- Concern for data leaks [maybe there should be even more concern …]
- Concern for ensuring availability in all situations
- Regulation

Implications of the Trends

- An encrypted packet is headed to Amazon cloud, how much can we learn from that?
- Increasing concern for sharing data or control, for various reasons
- Need to support highly bandwidth- and latency-intensive applications for a large fraction of the population
  - Today this is streaming and videoconferences

Current State

Reviewing past practices:

- ~~Name- and address-based policies~~
- ~~Protocol message analysis and modification~~
- ~~Content or deep packet inspection-based policies~~
- Traffic flow analysis
- Interactions based on explicit agreements and signalling
- Purely business- and agreement-level arrangements
- No interaction

Current State – Now What?

Key takeaways:

- The sooner we adapt to the new situation the better
- Interaction is not impossible, just different
  - Must find cases where there are mutual incentives
  - New methods may be technically different from past ones
  - Must be able to show there is no privacy or other concern
  - Not all past functions are feasible in new situation
- Decide where interaction is actually needed
  - Is it worthwhile in all situations?
- An opportunity for redesign – better, more secure, and mutually beneficial

Are There Opportunities in Interaction?

Should we still have interaction, given all these issues?
Yes – there are many areas where interaction could be beneficial:

- Networks understand the state of a path, can we use that?
- Applications understand their needs and network experience, can we use that?
- Can we continue managing, debugging, or tuning the networks?
- Could integration of network, cloud, and application processes lead to optimizations?
- Is there a need to share energy consumption information?
- Can applications use future network features such as sensing?
- Can we make network features more accessible to wider variety of applications?
- Can new technologies such as privacy-preserving measurements be used?

Potential Guidelines 1

GUIDING PRINCIPLE	WHAT	EXAMPLES
Intentional distribution	Per RFC 8558	Bad: middlebox reads TCP options Good: ECN
Minimal set of entities	Limit exchange to those with need to know	Bad: cleartext DNS query Good: encrypted query
Minimum information	The info that is needed for the task	Bad: user's or application's identity Good: describing sender's QoS preferences
Consent of parties	Sender, recipient, and ultimately user willingness	Bad: must disclose user id, or must process hop-by-hop header Good: Application decides

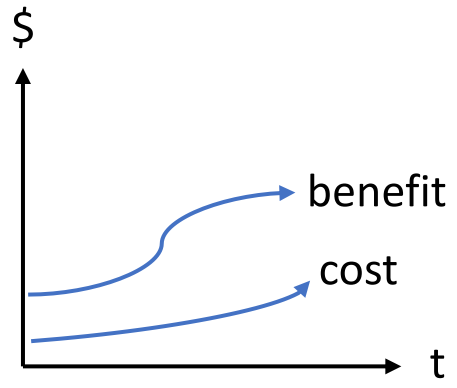
Potential Guidelines 2

GUIDING PRINCIPLE	WHAT	EXAMPLES
Securing the signals	Does the information need to be protected? Do the parties need to be authenticated?	Sharing simple data (e.g., ECN bits) Sharing sensitive data (e.g., DNS) Authentication may not imply trust
Pick the right ”layer”	Consider what approach works well	Signalling a need vs. Fixed subscription satisfying that need vs. Application dynamically adjusting to bandwidth needs & availability
Align the incentives	Do all parties have incentives for this approach?	TTM in changing applications vs. changing many networks in the world

Some Practical Examples

- ECN bits, Spin bit – benign and well-analysed information, beneficial
- Carrying user or application identity information – problematic in many ways
- Networks taking on application-oriented tasks, e.g., load-balancing decisions instead of just forwarding – unlikely to work well
- Fragmented ecosystem for accessing whatever interaction there is – unlikely to be broadly used, but unified or aggregated one could be
- How to start using holographic communication?

More about Incentives



Failures

- Chicken-and-egg: no usage – implementations – support
- A party needs to participate but has no reason to
- Too complex or costly

Successes

- Address a critical current problem
- Positive net value
- Incremental deployability
- Open code, spec, and process
- Sufficiently good solution

Incentives for Interaction

- Obviously at least two parties – must have incentives for both
- Likely needs to address an immediate problem for both
- Both parties must find the same solution optimal
- Avoid potential risk factors or additional dependencies
  - Lose visibility, make debugging difficult, require changing end-user contracts, require contracts with third parties, etc.

What NOT to Do

- Think that networking experts alone can do this, without collaborating with application experts
- Ignore potential misuse cases, e.g., applications are unlikely to wish to engage in activities that could be used for filtering such applications
- Ignore security issues, surveillance, or providing control to new parties
- Believe that networking layers can solve all issues
  - Typically, much more information held by applications, cloud platforms, etc.
- Expect all applications to contract with all networks

Challenges

- Information sharing
  - How can we maintain observability across all the systems?
  - How can we access or share measurement data?
  - What are the right interfaces between network, cloud, and application?
  - Sharing information from networks to applications? What state info can be safely shared?
- Security
  - Secure communications with multiple network elements, in multiple different networks?
  - Can we protect information held by network or servers, beyond communications security?
- New applications for interaction
  - Could network-application interaction help combat denial-of-service attacks?

Related Work at the IETF, IAB, and IRTF

- RFC 5218 – protocol deployment incentives
- RFC 8546 – wire images
- RFC 8558 – explicit signals
- RFC 9049 – what not to do
- Draft-iab-path-signals-collaboration – guidelines
- IAB M-TEN workshop (October) – management in an encrypted world
- IAB E-IMPACT workshop (December) – environmental impacts

Questions and discussion welcome!