Supporting More Dynamic Service Agreements

Ken Calvert

University of Kentucky

calvert@netlab.uky.edu

Agenda

I. Background (3 min)
II. In-band mechanism: FPAC (4 min)
III. Control-plane approach: "Coin-operated" ESDX (5 min)
IV. Other related work (2 min)

Background

General Theme: Making the network service and ecosystem more dynamic.

- Active Networks (late 1990's-early 2000's)
  - Ephemeral State Processing
  - Concast = inverse multicast service
- Postmodern Internet Architecture (NSF FIND, mid-late 2000's)
  - Clean-Slate design – Source Routed network layer
  - Explicit "Motivation" and "Accountability" fields carried in packet header
- ChoiceNet (NSF, grafted onto FIA program, 2010's)
  - Idea: encourage competition by providing mechanisms to support dynamic choice by users (including compensation)
  - "Economy Plane" for the Internet
- Economic Software-Defined Exchanges (ESDXs)
  - Exchange points as trusted arbiters between ISPs

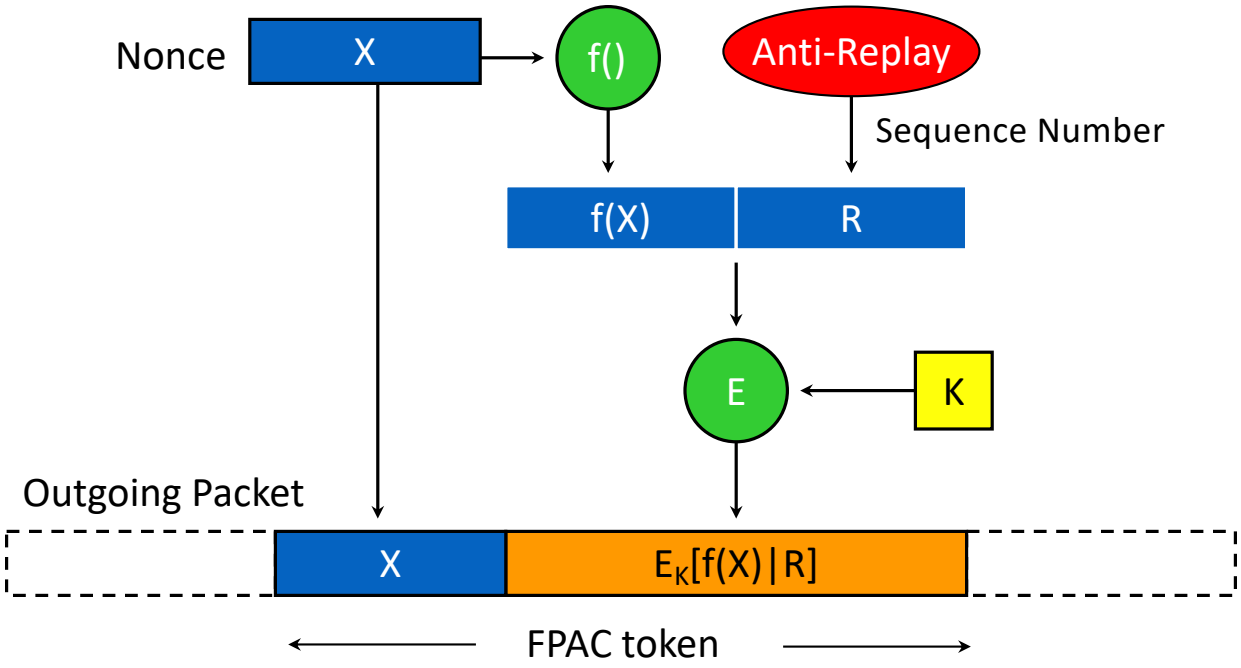
FPAC: In-band Access Control for Enhanced Services (Infocom 2002)

- Traditional approach to enhanced services:
  - Access (to reserved bandwidth, buffering) via packet classification
  - Based on unauthenticated header information
    - IP addresses, port numbers
- Problem: Spoofed packets can usurp limited resources
  - Difficult for providers to "guarantee" quality
- Goal: lightweight, hard-to-spoof credential
  - Fixed-cost, implementable at line speed (at least at borders)
  - Tied to packet to prevent re-use
- Assumes:
  - Shared secret between Sender and Verifier
    - Established out-of-band via signaling
  - Routers not compromised

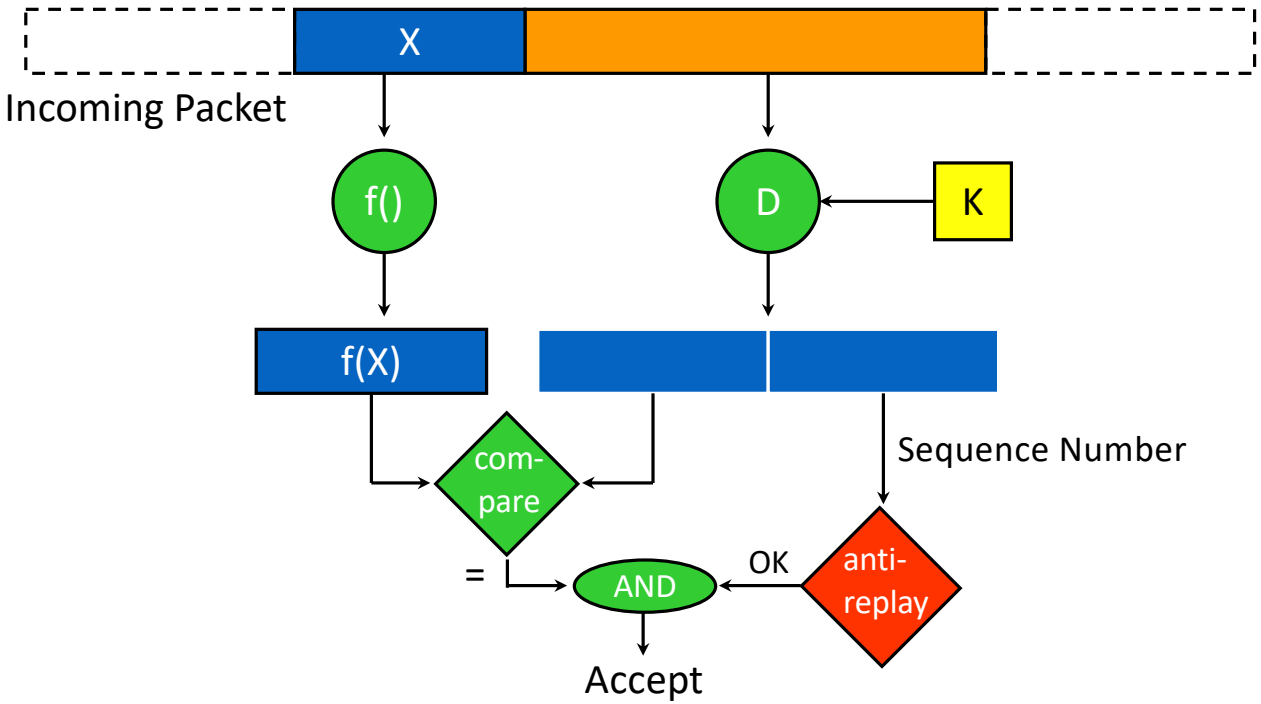
FPAC: Fast Packet Authentication Code

- Want origin authentication + anti-replay
- Approach: encrypt nonce under a secret key with block cipher; send nonce with ciphertext
  - Observation: Absolutely airtight security not required.
- Design challenges:
  - Hard to forge
  - Key distribution (cf. SCION)
  - Prevent replay
  - Authenticate with a single ~fixed-cost operation
- Two versions
  - Unattached (described here) – not tied to payload
  - Attached – credential weakly tied to packet content

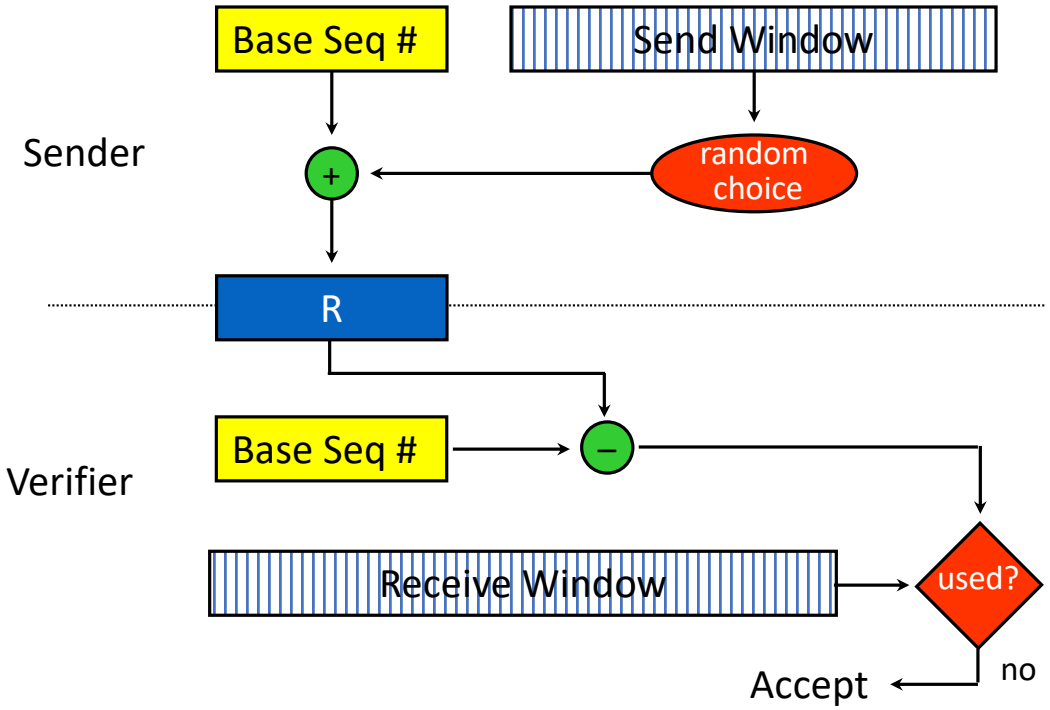
FPAC: Sender Computation



FPAC: Verifier Computation

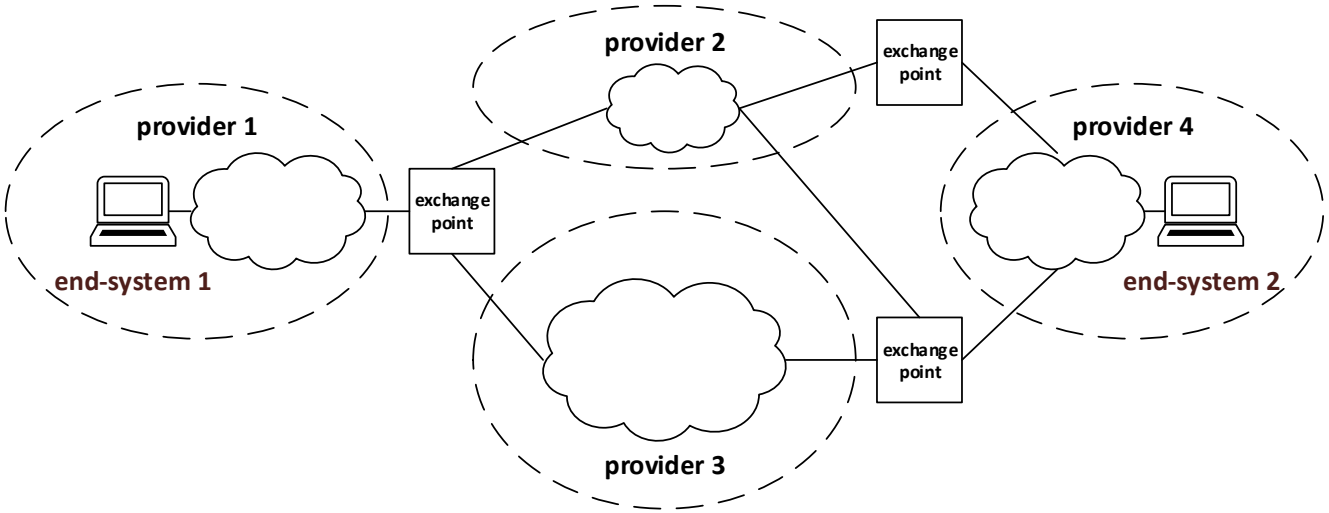


FPAC: Anti-Replay Mechanism



Interdomain Routing

- Today: packets follow money
  - Money flow changes slowly
  - BGP = the most-ossified interface?
- Goal: Enable more dynamic money/packet flow
  - Support shorter-term, dynamic contracts

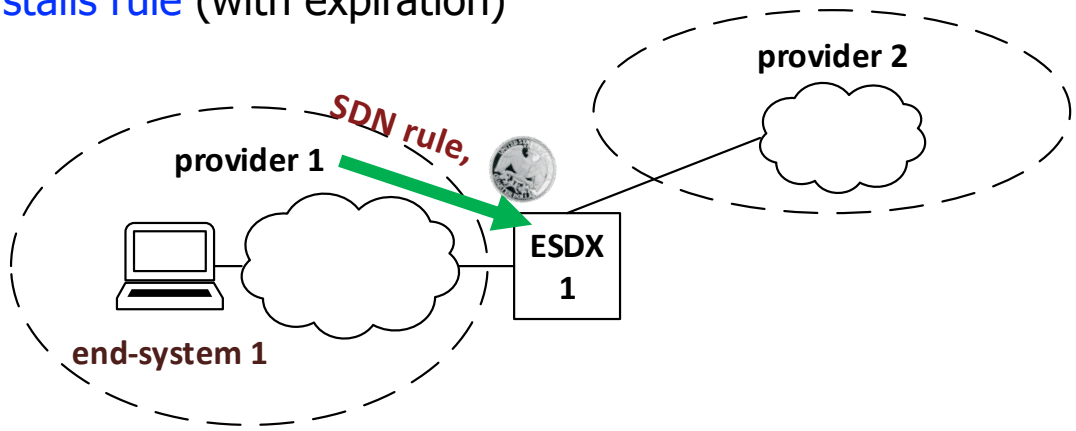


IPXs and SDN

- Economic Software-Defined Exchange Points (ESDXs)
  - Dynamic creation of granular forwarding rules
  - Acts as trusted intermediary between providers
    - Establish dynamic peering agreements between providers
    - Enforcing routing policies between providers
- Building block: "coin-operated" ESDX
  - "Pay" for rule insertion into SDX
  - Basis for economic agreements between providers
- Allows for finer-grained rules at shorter timescales
  - Enables short-term, on-demand agreements between providers
  - Enables control for end-to-end network connections

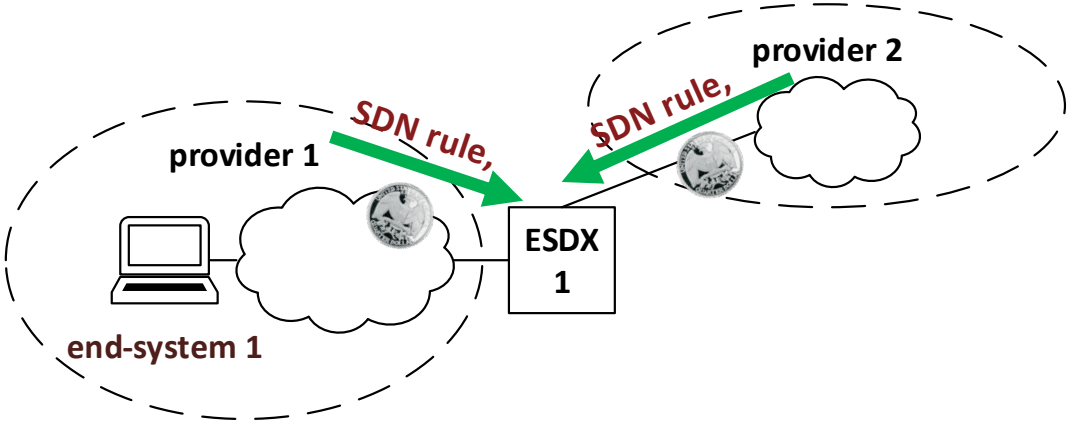
Economic SDX

- Coin-operated ESDX
  - Provider requests installation of SDN rule in ESDX
    - Sends SDN rule (k-tuple [+]) to ESDX
    - Sends coin (cryptographically signed certification) as payment
  - ESDX response
    - Verifies coin
    - Verifies rule (e.g., relates to this provider, not other providers)
    - Installs rule (with expiration)



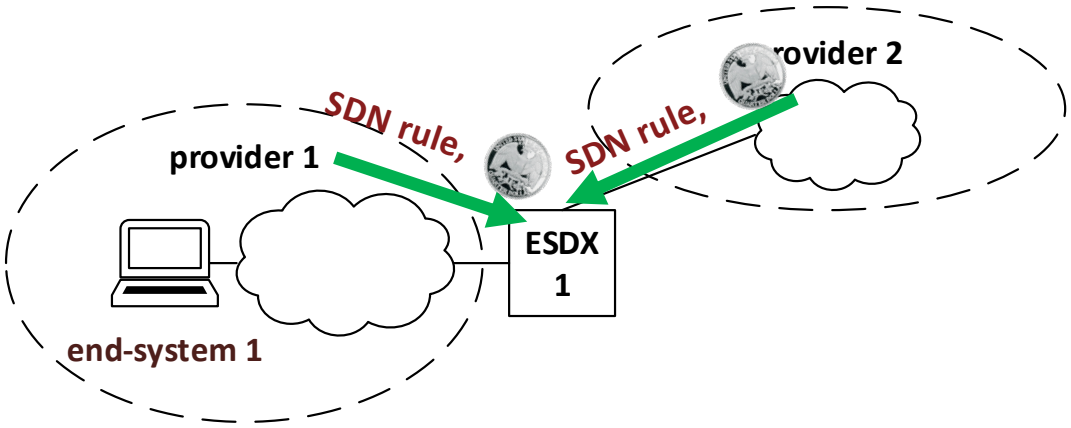
Economic SDX

- Bilateral agreements
  - Two providers request "matching" rule installation
  - ESDX installs both rules to connect providers
  - ESDX acts neutral party that enforces agreement
- Example:
  - Provider 1: Send egress (128.119.*,128.171.*) traffic to Provider 2
  - Provider 2: Receive ingress (128.119.*,128.171.*) traffic from Provider 1



Economic SDX

- Bilateral agreements
  - If rules are not exact match, then intersection is installed
- Example:
  - Provider 1: Send egress (128.119.*,*) traffic to Provider 2
  - Provider 2: Receive ingress (*,128.171.*) traffic from Provider 1
  - ESDX installs rule for (128.119.*,128.171.*)

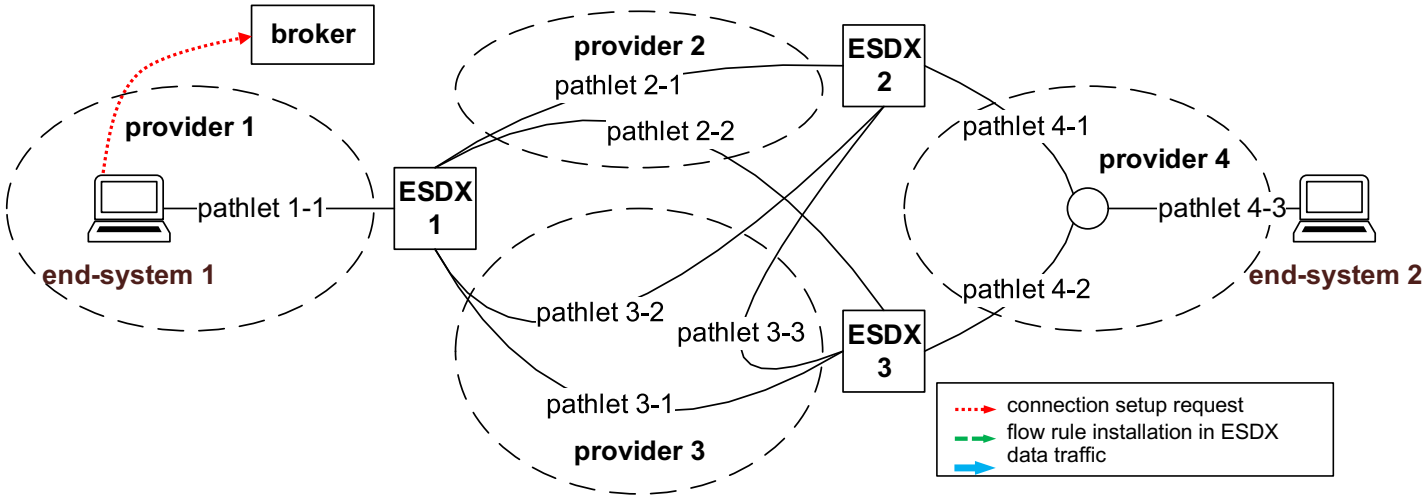


ESDX Rules

- Off-by-default is baseline for ESDX
  - No traffic is forwarded without explicit rule (similar to SDN)
- Rules are constrained to the requesting provider
  - Providers can only influence their own traffic
- Rules might specify QoS parameters
  - Allocated bandwidth
  - Total transmission amount
  - Might be policed if switch/network capabilities allow
- Rules are time-limited (or traffic-amount-limited)
  - Need new rule installation after expiration
    - Ensures that both sides of bilateral agreements still agree
    - Ensures that ESDX receives continued payment
  - Enables easy changes if desired

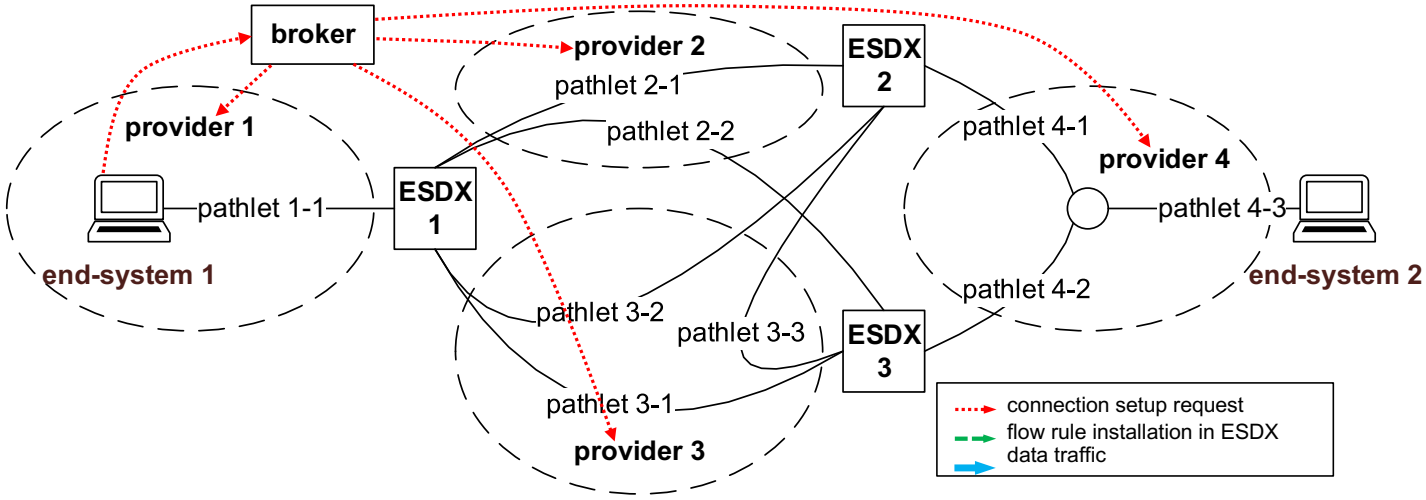
End-to-End Connections with ESDX
(See ICDCS 2019 "Spot Market" paper)

- "Brokers" can act as intermediaries for end-to-end paths
  - Edge provider pays broker to coordinate rule setup between providers
  - Broker pays providers to install suitable rules
  - Providers pay ESDX for providing connection
- Complete ecosystem where money flow aligns with traffic



End-to-End Connections with ESDX
(See ICDCS 2019 "Spot Market" paper)

- "Brokers" can act as intermediaries for end-to-end paths
  - Edge provider pays broker to coordinate rule setup between providers
  - Broker pays providers to install suitable rules
  - Providers pay ESDX for providing connection
- Complete ecosystem where money flow aligns with traffic



Other Possibly Relevant Work

- SCION (Perrig 2017) – Complete design of a secure inter-domain network architecture.
- Chen's Thesis (UMass 2015) – OrthoCredential, another in-band authentication scheme based on Hadamard Matrices.
- Pathlets (Godfrey et al 2009) – another inter-domain routing architecture, source-routed.
  - Trust structure/authentication?

References

- FPAC: K. L. Calvert, J. N. Griffioen, S. Venkatraman, "Authenticated Access to Reserved Resources", *International Journal of Network Security*, 3(1), July 2006, pp. 54–64.
- ChoiceNet: X. Chen, T. Wolf, J. Griffioen, O. Ascigil, R. Dutta, G. Rouskas, S. Bhat, I. Baldin, K. Calvert, "Design of a Protocol to Enable Economic Transactions for Network Services", *Proceedings IEEE International Conference on Communications (ICC)*, London, UK, June 2015, pp. 5354-5359.
- ChoiceNet: T. Wolf, J. Griffioen, K. Calvert, R. Dutta, G. Rouskas, I. Baldin, and A. Nagurney, "ChoiceNet: Toward an Economy Plane for the Internet", ACM SIGCOMM *Computer Communication Review*, Volume 44, Issue 3, July 2014, pp. 87–96.
- ESDX: J. Griffioen, T. Wolf, K. Calvert, "A Coin-Operated Software-Defined Exchange", Proceedings of 2016 International Conference on Computer Communications and Networks, August 2016, Hawaii.
- ESDX: K. L. Calvert, J. Griffioen, A. Nagurney and T. Wolf, "A Vision for a Spot Market for Interdomain Connectivity", 39th IEEE International Conference on Distributed Computing Systems (ICDCS) Blue Sky Track, July 2019, Dallas, TX.
- PoMo: J. N. Griffioen, K. L. Calvert, O. Ascigil and S. Yuan, "Separating Routing Policy from Mechanism in the Network Layer", in *Next-Generation Internet Architectures and Protocols*, B. Ramamurthy, G. Rouskas and K. Sivalingam, eds., Cambridge University Press, 2011.
- ESP: K. L. Calvert, J. N. Griffioen, S. Wen, "Lightweight Network Support for Scalable End-to-End Services", *Proceedings ACM SIGCOMM 2002*, Pittsburgh, August 2002, pp. 265–278.
- Chen, Xinming, "Design and Implementation of an Economy Plane for the Internet" (2015). Doctoral Dissertations. 487. https://doi.org/10.7275/7497694.0 https://schlarworks.umass.edu/dissertations_2/487