Poster: NDN+SCION: Global Name-based Routing

Ken Calvert
University of Kentucky
calvert@netlab.uky.edu

Jeremiah Davis
University of Kentucky
jeremiah.davis@uky.edu

***Abstract*—A practical inter-domain routing and forwarding system remains an open challenge for Named-Data Networking (NDN). At the same time, SCION is an emerging path-aware inter-domain routing and forwarding system designed to improve on the current Internet's BGP-based system in several ways. Both NDN and SCION emphasize end-to-end security and trust, while also offering multipath capabilities. This leads us to consider network layer based on named data that uses NDN for intra-domain routing and forwarding, and SCION for inter-domain. Among the challenges to be overcome are where to implement the intra/inter-domain protocol transition, and how to scale the system to handle the vastly larger namespace of NDN. We describe a preliminary approach and lay out some key research questions.**

I. Background

The named-data networking (NDN) protocol provides retrieval of data objects via hierarchical names. Importantly, it also enables verification of *origin authenticity* of all returned data, based on its (application chosen) name, as each object is cryptographically signed. The secure binding between name and data object enables applications to define their own *trust structures*, i.e., the naming pattern that enables the recipient of a data object to determine that it was created/signed by a trusted source.

An unresolved question for information-centric networking in general is the design of a scalable inter-domain routing (IDR) system. The legacy IDR system based on BGP is not suitable, for two reasons: (i) sources of named data need not be tied to specific network locations the way IP addresses are (indeed, this is the point of information-centric networking); and (ii) the set of potential application names is unbounded. Although a number of solutions have been proposed, none has emerged as a satisfactory candidate [1], and NDN deployments, including the NDN testbed [2], operate as single-domain *overlays* on the current Internet.

SCION [3] is an emerging path-aware inter-domain routing and forwarding system that does *not* depend on BGP. It is designed to overcome security limitations of BGP and IP while maintaining policy-compliance, enabling multi-path forwarding, and not requiring reliance on a single global root of trust. In SCION, autonomous systems (ASes) organize themselves into regions called isolation domains (ISDs), each with a common root of trust. Designated *core* ASes provide connections to other ISDs. Core ASes flood beacon packets, which build up *AS paths* as they are forwarded (according to policy) throughout the ISD; paths are eventually collected by a *path service* for the ISD. Packets that cross AS boundaries are source-routed and carry an AS path containing cryptographic proof of policy-compliance. Thus, SCION is a purely inter-domain routing/forwarding service, which *in principle* is independent of any intra-domain forwarding protocol.

979-8-3503-5171-2/24/$31.00 ©2024 IEEE

Both of these protocols should (at least in principle) be able to operate directly on Layer 2, without dependence on IP routing and forwarding. Both support forwarding packets over multiple paths concurrently, optionally under application control (at least in theory). They provide complementary functions, with an emphasis on security as a primary design objective. The high-level objective of our project is therefore to combine NDN and SCION to form a scalable global network protocol and service that is completely independent of IP—i.e., *not an overlay*.

II. Design Goals

We have the following design objectives:

- **NDN intra-domain.** Within origin and destination ASes, forwarding is based on the NDN architecture *only*: Interest packets (requests for specific named data objects) are routed based on hierarchical names, while each Data packet follows the reverse path to the origin of the eliciting Interest, following temporary "bread crumb" state left by that Interest at routers. Transit ASes can tunnel packets (using any protocol) between border routers.
- **Protocol compatibility.** As far as possible, existing NDN and SCION protocols should be used without modification. (Of course, additional components may be required.)
- **Multipath.** Both NDN and SCION allow a host to choose among multiple forwarding paths and to use more than one path concurrently. The design should preserve this capability and expose it to path-aware application endpoints.
- **IP-independence.** The system should not rely on IP at any point in the design.
- **Flexible trust structure.** No part of the system should require universal agreement on a *single* root of trust (unlike DNS and BGP/IP). In particular, applications can specify their own rules about which sources are authoritative for which parts of their namespace.
- **Trustworthy routing.** To avoid wasting resources, the IDR system must ensure that Interests are only forwarded toward sources that can produce *authentic* Data with the given name. Therefore, the IDR system must have some way of verifying a source's legitimacy *according*

to the application trust structure, before propagating information about it in the control plane.

Some of these goals are in tension, if not outright conflict. For example, consider the requirement that applications be free to define their own trust structures (cf. the current one-size-fits-all Web trust structure), versus the goal of only propagating information about legitimate sources of data. It is simply not reasonable to require the network infrastructure to be aware of application trust structures, or to propagate information about an unbounded number of trust roots globally. Thus, some additional mechanism or intermediary is required.

III. Research Questions

A. NDN+SCION boundary location

NDN and SCION use different forwarding protocols. Where should protocol translation and encapsulation occur—at the originating host, at the first egress router, or somewhere in between? This question has implications for the service's interface to applications. We would like to allow for both SCION (multi-)path-aware and traditional NDN applications.

B. Application vs. Network Trust

Where and how do the application and network trust regimes intersect? Network trust is slow-changing, based on peering agreements among ASes, some of which involve payment, while application trust is much more ephemeral and granular. At minimum, the network should be able to verify the legitimacy of a putative source without requiring global propagation of the entire application trust structure.

C. Routing Information Scope

What information is propagated globally, and how? NDN uses location-independent identifiers. SCION uses identifiers tied to specific locations. The system must have a way to map names in Interests to (sets of) ASes known to contain legitimate sources of data with that name. In the current Internet, the combination of BGP, hierarchical DNS names *with a common root*, and the use of anycast addresses for root zone name servers enables name-to-location resolution for a potentially unbounded number of "application" names (think URLs), by propagating about 1.3 million IP address prefixes globally, way ahead of time [5]. The SCION protocol, on the other hand, floods *path-construction beacon* packets along policy-compliant paths and only *within* ISDs. The question is how much name prefix-to-AS mapping mapping should be propagated ahead of time, versus on demand.

IV. Outline of an Approach

The NDN architecture places the name-to-location resolution function to within a "strategy layer", which is responsible for choosing (or discovering) a path along which to forward each Interest, and possibly adapting that path based on real-time feedback. We propose to handle the intra/inter-domain routing transition *within the strategy layer*. Carefully designed signaling mechanisms in this interface can enable applications to take advantage of the multipath capabilities of *both* NDN [10] and SCION, to discover if multiple paths are available and their characteristics, and to indicate which paths to use in real time (e.g., based on observed metrics). Ideally, this interface could be designed to function whether the name-to-location resolution (and thus the intra/inter-domain transition) is at the local host or at a downstream node in the same AS. This approach means that NDN applications would not need to be rewritten to be SCION-aware.

Rather than propagate application name prefixes globally between ASes (*a la* BGP), we propose to push the function of locating data sources at the inter-domain level to a separate service. SCION has a secure name resolution system called RHINE [6], which is designed to improve on today's DNS in several ways, including by supporting more general approaches to delegation of authority. The NDN strategy layer can use this service to locate legitimate sources (destinations for Interests), provided Data sources register their prefix and location with the name service. We expect that sources would execute a transaction with a name server to prove their authorization to produce named content in that AS and namespace in the process, using something like RICE [8] or reflexive forwarding [9].

However, unlike the DNS, which has a single, globally well-known starting point for name resolution, namespaces in our system may have many roots. Thus, applications need a way to locate the root name server(s) for their specific trust root context. Moreover, as noted above, the number of distinct namespace roots needs to be constrained somehow. Our solution is to require that each application namespace root of trust—uniquely identified by, say, a public key hash plus an encoded *trust schema* [7]—operate a globally distributed set of *top-level name servers* for its namespace. (This operational requirement is analogous to ICANN funding today's DNS root servers by the fees paid to lease zones in the DNS.) We expect this requirement to constrain the number of global trust roots. Note that local applications, such as home automation or enterprise data services, need not and *should not* be visible in the global routing system.

In addition, every AS runs a *rendezvous service*, which collects information about any namespaces top-level root servers are located within that AS. That information (namespace root-to-AS mappings) is then gossiped among ASes in the ISD in the same general way that AS-path information is collected and propagated in SCION. The rendezvous service enables application endpoints, upon startup, to find a name server for their particular namespace, and (recursively) resolve their application prefix either to sources of data, or name servers with which to register. This is where the network and application trust regimes intersect; thus, the rendezvous service should also play a role in enabling an AS to verify a source's claimed legitimacy within a namespace. Design of this global verification system so that it scales to securely handle classes of application ranging from mobile telephony to the world-wide web is a major challenge of this project.

REFERENCES

[1] J. S. Davis and K. L. Calvert, "SoK: On Named Content and Interdomain Routing", *Proceedings ACM Conference on Information-Centric Networking (ACM ICN 2024)*, Reykjavik, Iceland, October 2024.

[2] L. Chuat et al, *The Complete Guide to SCION*, Springer, 2022.

[3] https://named-data.net/ndn-testbed/, accessed 12 August 2024.

[4] SCION Association case study. https://www.scion.org/ssfn-scion/, accessed 12 August 2024.

[5] Cloudflare Radar. https://radar.cloudflare.com/routing, accessed 12 August 2024.

[6] H. Duan, R. Fischer, J. Lou, S. Liu, D. Basin and A. Perrig, "RHINE: Robust and High-performance Internet Naming with E2E Authenticity", *Proceedings of NSDI 2023*, April 2023, Boston, USA.

[7] Y. Yu, A. Afenasyev, D. Clark, k. claffy, V. Jacobson and L. Zhang, "Schematizing and Automating Trust in Named Data Networking", *Proceedings of the ACM Conference on Information-Centric Networking* (ACM ICN 2015), September 2015.

[8] M. Król, K. Habak, D. Oran, D. Kutscher and I. Psaras, "RICE: Remote Method Invocation in ICN", *Proceedings of the ACM Conference on Information-Centric Networking* (ACM ICN 2018), September 2018.

[9] D. Oran and D. Kutscher, "Reflexive Forwarding for CCNx and NDN Protocols", Internet Draft draft-oran-icnrg-reflexive-forwarding-05, March 2023.

[10] I. Moiseenko and D. Oran, "Path switching in content centric and named data networks", *Proceedings of the 4th ACM Conference on Information-Centric Networking*, September 2017.