Recent Advances in Named Data Caching and Routing

Mohan Li, mohan.li (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain) Download

Abstract:

This paper presents recent advances in the research on named data caching and routing since the Named Data Networking (NDN) project's initiation in 2010. NDNâ€™s in-network caching feature enables opportunities to significantly reduce network bandwidth usage while causing series of security and privacy concerns. In this paper, related work on caching schemes are presented and cache attack patterns and countermeasures are discussed. Routing in NDN differs from IP-based routing fundamentally and great research efforts have been put into this topic. General discussions on Inter-ISP (Internet Service Provider) routing policies in NDN are first summarized. As for intra-ISP routing, the evolution of NDN routing protocols from the temporary extension of OSPF (Open Shortest Path First protocol) to long-term deployment of NLSR (Named Data Link State protocol) is described. Other proposals such as the 2-layer routing hierarchy and controller-based routing scheme are also discussed.

Keywords:

Named Data Networking (NDN), Content-Centric Networking (CCN), NDN Caching, Caching Scheme, Privacy and Security, Attacks and Countermeasures, NDN Routing, Routing Policy, Routing Protocol NDN Forwarding, OSPF, OSPFN, NLSR

Table of Contents:

- 1. Introduction
- 2. NDN Architecture and Research Agenda
  - 2.1 Architecture Design
  - 2.2 Research Agenda
- 3. NDN Caching
  - 3.1 Caching Schemes
  - 3.2 Security and Privacy
- 4. NDN Routing
  - 4.1 Inter-Domain Routing Policies
  - 4.2 Intra-Domain Routing Protocols
- 5. Summary
- 6. List of Acronyms
- 7. References

1. Introduction

The last several decades have witnessed the success of the Internet facilitated by the IPâ€™s ubiquitous connectivity. But todayâ€™s mainstream network usage has shifted from the original point-to-point (P2P) conversations to massive content creation and distribution. This means todayâ€™s Internet users care more about what the content they want is rather than where the content they requested is located. Such fundamental change exposes the limits of the IP-based network and poses several challenges as well as opportunities that drive the initiation of the NDN project.

The NDN project is designed to take advantage of many new opportunities [Zhang10]. First, NDN can avoid the complex middleware used in IP-based network that maps the content to its location. Second, instead of the â€œone-fits-allâ€ security policy IP can provide, NDN can deploy finer-grained security strategies that authenticate the data by signature. Third, in NDN, every chunk of data is uniquely named so that data packets can be forwarded using multiple paths, removing IPâ€™s single-path forwarding constraint.

On the other hand, the challenges faced by NDN are also intriguing [Zhang10]. First, NDN needs an IP Address like hierarchical naming scheme to enable â€œscaling via aggregationâ€. Second, wire rate forwarding has been a research issue for decades. NDN should take advantage of recent techniques and achieve wire-rate to forward the names. Third, security issues should be taken into consideration more inherently while developing NDN than developing IP networks decades ago.

The NDN project emphasizes its compatibility with the existing IP-based network. NDN is designed to share the universal overlay property of IP so that it runs over any networks and vice versa. The developers envision NDN as efficient in content distribution, friendly to application development and built-in support for security and smooth for mobility.

The rest of the paper is organized as follows. Section 2 provides backgrounds of NDN necessary for the topics covered in this paper. NDN architecture design issues and research agenda are presented. Section 3 covers NDN caching issues including caching schemes and potential security and privacy issues caused by NDN caching. Section 4 presents researches on NDN routing including routing policies, routing protocol evolution and proposals. Section 5 summarizes the paper.

2. NDN Architecture and Research Agenda

The duality within NDN lies in that it is a fundamental paradigm shift from the IP-based Internet while it is designed to be compatible and can run over the current network. Therefore, NDN architecture has to be designed carefully to balance the tradeoff between innovation and compatibility. Section 2.1 covers NDN architecture design principles and reasoning.

As NDN is designed to be a brand new network architecture, there are a lot of research issues that need time and effort. Therefore, various topics must be carefully prioritized to reflect the urgent needs of a network prototype while maintaining focus on vital research issues. Section 2.2 presents the NDN research agenda and points out the caching and routing issues within.

2.1 Architecture Design

There are two aspects worth considering on the principles of NDN architecture. On one hand, NDN is supposed to be a brand new architecture that should take a giant leap from the one of the current Internet. On the other hand, NDN should be practical and be compatible with the current IP-based network. With such thoughts in mind, the NDN architects designed the network framework with the following principles.

First, NDN should share the elegant hourglass structure with the IP. The hourglass architecture only requires minimal functionality while enabling universal connectivity. Second, the separation between forwarding plane and routing plane has been proven necessary to allow forwarding to keep functioning while the routing schemes continue to develop. NDN should maintain such separation and allow researches on forwarding and routing to be conducted in parallel. Third, rather than an after-thought, security should be built in inherently within NDN and all data packet should have a signature. Last, the traffic flowing in NDN should be self-regulating. In other words, traffic should be kept flow-balanced in NDN [Zhang10].

In NDN, the data consumer drives the communication. A consumer sends out an "Interest" packet to request data. The Interest packet carries the requested data name and the router looks the name up in its Forwarding Information Base (FIB). A Data packet is sent back once the forwarded Interest packet reaches a router that has the data that matches the name. The routers also keep the Interest packet and Data packet for a while and when there are multiple Interests arriving at a router, it keeps them in the Pending Interest Table (PIT). Data are kept in the Content Store (CS) to speedup future requests. The Interest and Data packet format are shown in Figure 1. [Zhang10].

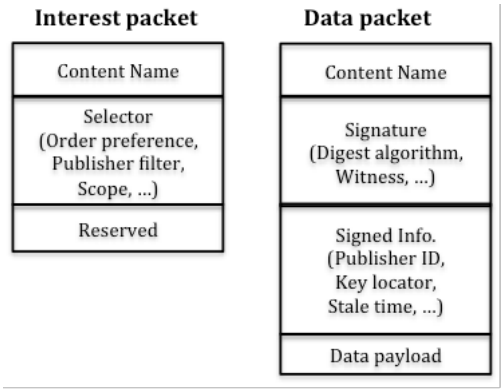


Figure 1. Packets Format in NDN Architecture

The content router first checks for the availability of the requested content in its CS when it receives an Interest packet. If the content is available (a cache hit), the CS sends the data back to the requester along the recorded reverse path. If not, the content router checks whether such content was requested previously and logged in its PIT. Recall that PIT is used to keep track of content items that were recently requested but were not sent back. If no entry is found in the PIT, a new entry is created and the Interest Packet is then forwarded to FIB. If a pending request is found and the Data packet of the target content travels from the source or cache downwards to the requester, the content routers on the path determine whether to replicate the content item according to the caching strategy. Such procedures are shown in Figure 2 [Li12a] and Figure 3 [Zhang10]. Thus designing effective caching strategies becomes one of the key issues in the area of NDN caching.

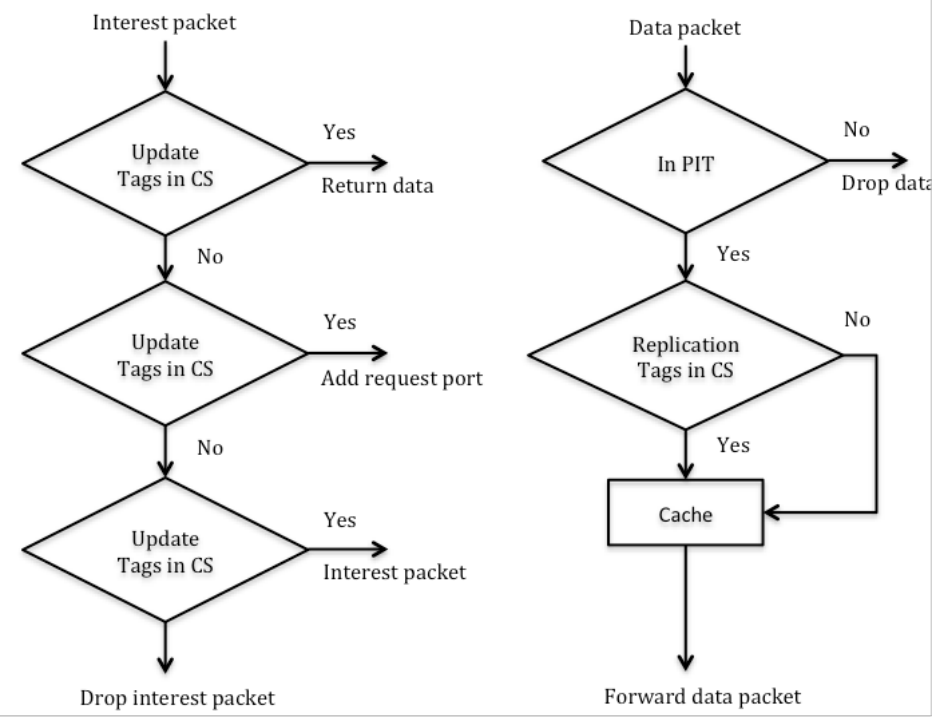


Figure 2. Forwarding and Caching Model

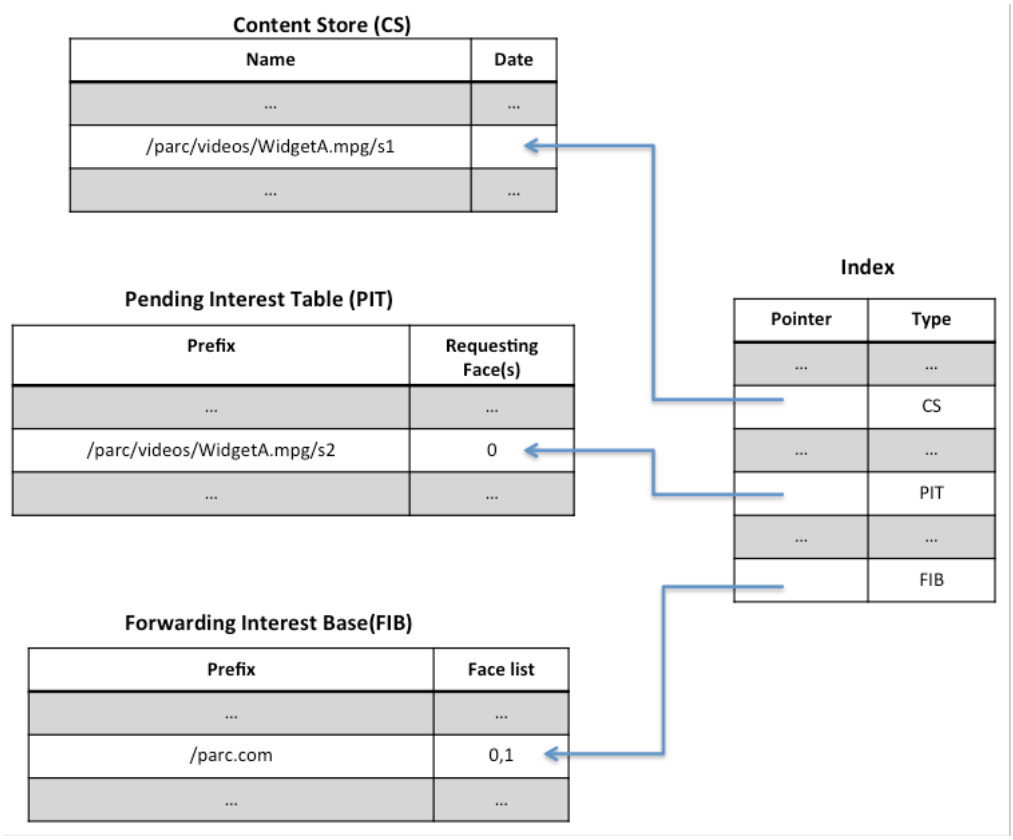


Figure 3. Forwarding Process in a NDN Router

The building blocks of NDN include the naming system for the data, data-centric security mechanisms, forwarding, routing and caching, transportation and data structure. NDN caching and routing will be covered and discussed in section 3 and section 4 respectively.

2.2 Research Agenda

NDN is a brand new network architecture proposal and it raises various kinds of challenges and also enables many opportunities that are difficult to provide in IP-based networks. Started in 2010, the NDN project is fairly young and there are many issues that need to be covered. Therefore, the NDN team has prioritized their research agenda and highlighted several topics that are vital and critical for realizing and testing the NDN design. These topics are listed as follows:

- Scalable routing solutions
- Fast forwarding engines
- Driven applications running on top of NDN
- Security foundations
- Verifications and evaluations

There are two major challenges in NDN routing. First, the amount of routing states needs to be limited while the naming space for data should be boundless. Second, multipath forwarding should be enabled to spread Interests more efficiently. The NDN team has planed both short-term initial deployment to extend existing routing protocol and long-term deployment to achieve scalability. In short term, the routing team extends the OSPF protocol to solve NDNâ€™s problem of lacking a routing plane that are necessary for other research. In the long term, two approaches representing two possible directions are to be investigated. The first approach is to explore ISP-based aggregation. The second one is to exploit the naming space and the NDN network structure to achieve scalability. The topic of NDN routing will be further discussed in section 4.

Forwarding is another critical issue in NDN. In the research agenda, forwarding needs to be re-engineered to enable fast name look-up, intelligent Interest forwarding and effective caching. Three requirements need to be met:

- Variable length, hierarchical names
- Fast updates to prefix table
- High capacity

NDN routers cache packets ubiquitously and enable re-use of data after the first forwarding. A cache hit means reduction in network bandwidth, which gives NDN a startup advantage against IP. Issues on caching that are worthy of investigation include:

- Cache replacement policies
- Stale data avoidance
- Cache pollution attack prevention
- DDoS attacks prevention

The topic of NDN caching will be further discussed in section 3.

Besides routing, forwarding and caching, the NDN team also needs to develop applications that motivate:

- Architecture development

- Prototype implementation
- Function and performance demonstration

The NDN team will focus on applications with increasing societal interests including:

- Web browser protocol handler
- Media streaming application
- Media-rich cyber-physical system supports
- Human-centric sensing applications

Moreover, security and privacy should be considered along with other topics. Rather than an after-thought, NDN keeps security in mind at the very beginning. Every NDN packet is bounded with a signature that can verify the provider of the content. Such basic feature provides inherent data integrity and origin authentication. However, more sophisticated mechanisms need to be designed to cope with the increasingly hostile environment in todayâ€™s Internet. These mechanisms include:

- Signature Efficiency
- Trust Management
- Network Security Defense
- Copyright protection and privacy

The issue of security and privacy is high relevant to NDN caching and is covered in section 3.2.

3. NDN Caching

Recall that upon receiving an Interest packet, a NDN router first checks its Content Store to see if there is data matching the name. The CS can be implemented in the routerâ€™s memory as cache. Unlike IP in which data packet cannot be reused after forwarding, NDN routers cache and identify data by name and can achieve high delivery efficiency. Due to the dominant position of caching in the architecture of NDN, it has been widely discussed topics in NDN project. In recent years considerable amount of research efforts have been conducted concerning NDN caching. Those efforts include popularity-driven coordinated caching, effective caching schemes minimizing inter-ISP traffic, data structure design for content caching management. These research advances will be discussed in section 3.1.

In todayâ€™s IP network, both what the data is and who is requesting it can be inspected maliciously and privacy is poorly protected. Since NDN explicitly names the data, it seems even easier to inspect what the data is. However, NDN hides the information about communication endpoints entirely, therefore, the privacy of the data consumer and provider are inherently protected. Nonetheless, caching the explicit data poses other kinds of privacy threats such as cache pollution attacks and cache snooping. Research efforts have been conducted to address such privacy concerns and develop possible countermeasures against various kinds of attacks. Other researchers focus on privacy implications of NDNâ€™s ubiquitous caching and the tradeoff between privacy protection and network performance as a whole. The above research advances will be covered in section 3.2.

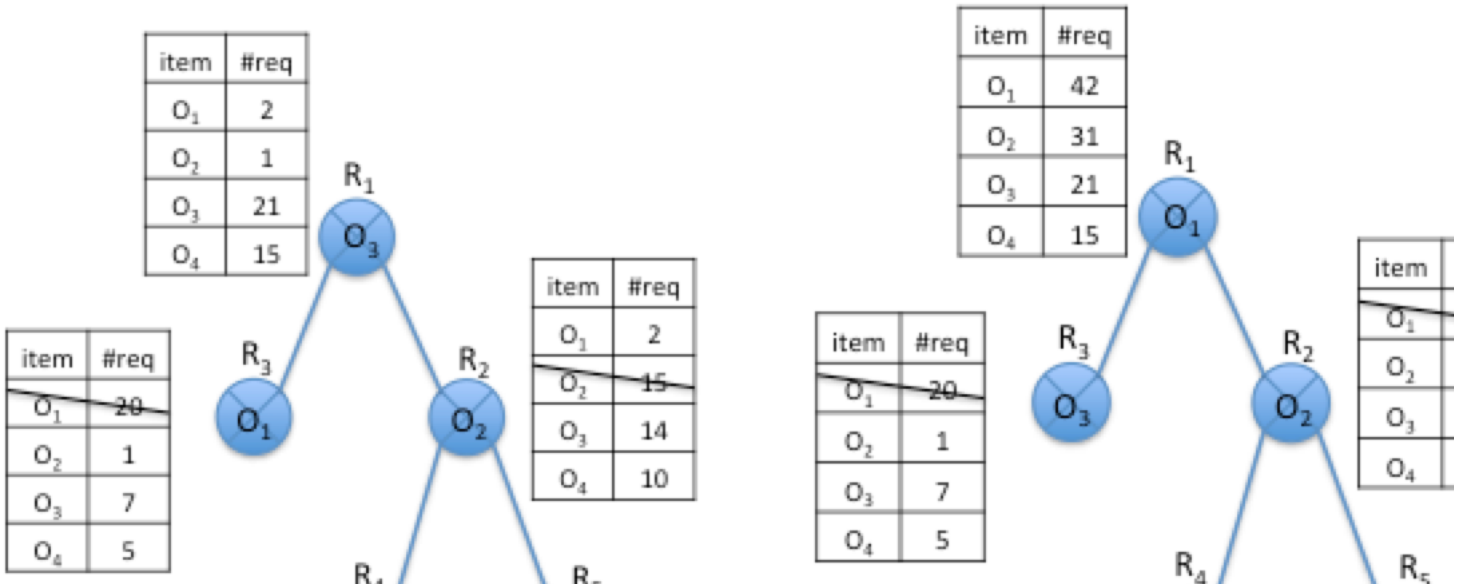
3.1 Caching Schemes

[Li12a] propose efficient caching schemes for ISPs to minimize the inter-ISP traffic. A caching system is proposed with its corresponding caching algorithm that dynamically determines cache replacement along the forwarding path. The researchers focus on effective caching schemes through carefully placing the content copies at appropriate in-network caches. The main contributions of their work are as follows:

- Design a dynamic caching system
- Present three coordinated caching algorithms: Top Down, Bottom Up and Bridging with online decision making
- Evaluate the performance of the above algorithms

In Bottom Up algorithm, each node makes its caching decision for each object according to the popularity measured by the aggregated request statistics of its own sub-tree. Its procedure is shown in Figure 4(a). The Top Down algorithm is illustrated in Figure 4(b). It gets sorted request records at each node by aggregating request records from bottom tier to up tier, till the root is reached.

Bridging algorithm, as the name implies, is to bridge Top Down and Bottom Up algorithms, aiming to take the advantage of them both. Following the basic caching principle of Top Down, Bridging draws the content with biased popularity distribution downwards to the end nodes without sacrificing the gain in inter-ISP traffic saving. Figure 4(c) shows how the Bridging algorithm works. Figure 4 references the work in [Li12a].



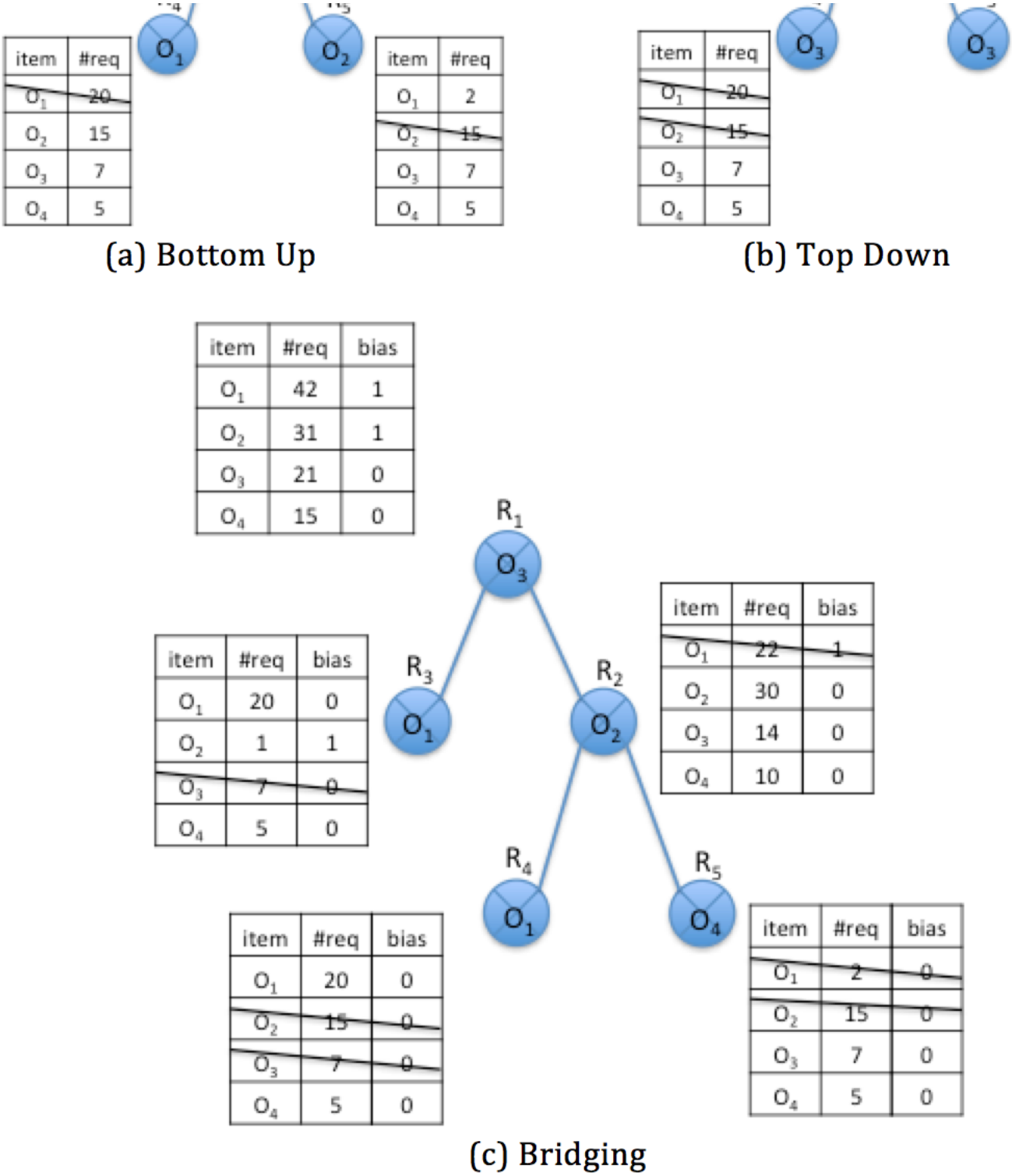


Figure 4. Illustration of the three Caching Algorithms

The simulation results show that the Bridging schemes outperform the widely used Leaving Copies Everywhere (LCE) both in inter-ISP traffic saving and the average number of access hops by up to 20%. Since even 1% reduction in inter-ISP traffic accounts for significant amount of traffic going through ISP boundary, such caching scheme is expected to benefit ISPs by sharply reducing costly inter-ISP traffic as well as easing the NDN deployment.

[Li12b] have also have developed a popularity-driven coordinated caching schemes to reduce the redundant traffic going through the NDN networks, trying to minimize both inter-ISP traffic and average number of access hops. The caching system can be modeled as a tree-like routing topology as shown in Figure 4. Two notations Level and Tier need to be clarified for such topology as shown in Figure 5. [Li12b].

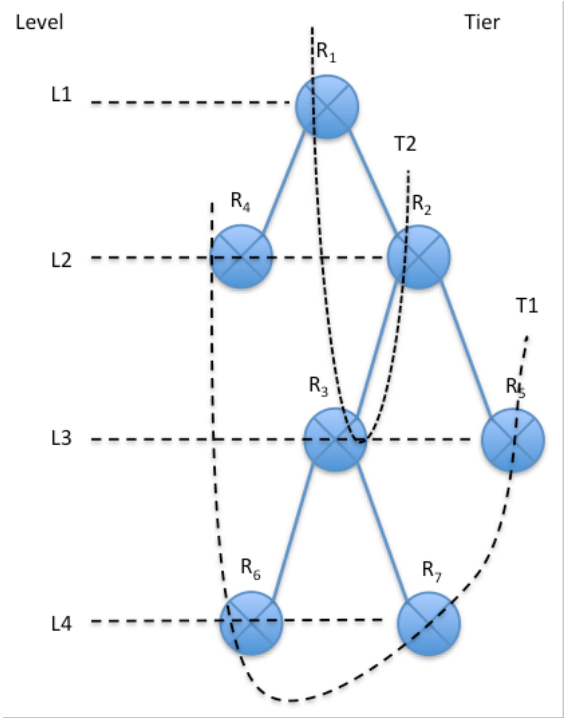


Figure 5. Illustration of Levels and Tiers

Tier is denoted as the distance from the intermediate node to the closest end node (each end node being T1), measured by the number of hops. The lower the tier, the closer it is to the end users. In contrast, Level is denoted as the distance from each node to the root R1 (R1 being Level 1), also measured by the number of hops. End nodes (nodes in T1) correspond to the highest-level caches and are responsible for monitoring the requests from the end users and the root node corresponds to the lowest level cache. The objects contained in the caches at the lower level can be shared and accessed by sub-tree nodes at higher level. A user request travels from an end node towards the root, until the requested object is found. Finally, if the requested content cannot even be found at the root tier, the request is redirected to the source content server that contains the interested object. Once the object is found, it is sent along the reverse path towards the requester. Each cache along the forwarding path independently decides the content replication according to a chosen caching strategy, which is determined by dynamic caching algorithms like the Bridged caching algorithm proposed in their previous work [Li12a]. The caching scheme achieves a performance close to the optimum with a favorable saving rate in inter-ISP traffic. It considerably improves the performance of access delay and intra-ISP link consumption measured by the number of hops traveled.

[Wang12a] describe a scheme on the cache memory management in CCN and explore its impact. To design a solution for the in-network cache, they set up an application platform using the open source CCNx prototype and redesign the cache management component by using the splay tree data structure and the according replacement policy.

The design follows the memory organization in todayâ€™s routers. The packets are stored in DRAM (main memory) and the index of the packets is stored in SRAM (CPU cache). The (packet, content) tuples (PIDs) in the index are organized as splay tree, which is a self-adjusting binary search tree. Such organization is shown in Figure 6 [Wang12a]. A splay tree has the function that recently accessed nodes are quick to be access again. Splaying the tree for a node rearranges the tree so that the node is arranged to the root of the tree. Thus, future access to this node will be faster. To perform this function, firstly it needs to perform a standard binary tree search for the node in question, and then use tree rotations in a specific fashion to bring the node to the top.

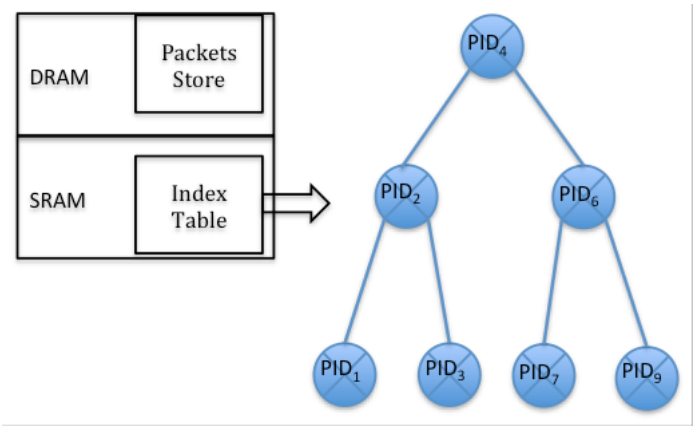


Figure 6. Cache Data Structure

The splaying tree structure proves to be suitable for caching for that recently accessed content is quick to access again. The researchers' experimental results show the high efficiency of management. The solution increases the hit ratio and takes less time to access popular content.

3.2 Security and Privacy

Router-side content caching optimizes bandwidth consumption, reduces congestion and provides fast fetching for popular content. Therefore it is considered one of NDN's key

feature. However, such feature is also detrimental to the privacy of both consumers and content providers. As shown in [Acs13], simple and difficult-to-detect timing attacks can exploit NDN routers as â€œoraclesâ€ and allow the adversary to learn whether a nearby consumer recently requested certain content. Probing attacks that target adjacent content producers can be used similarly to discover whether certain content has been recently fetched. After analyzing the scope and feasibility of such attacks, the researchers proposed and evaluated some efficient countermeasures that offer quantifiable privacy guarantees while retaining key features of NDN. First, it is suggested that consumers and producers should indicate which content is privacy-sensitive. Second, several techniques are provided to balance certain tradeoffs between privacy and latency. A formal model is also introduced that allows quantifying the degree of privacy offered by various caching algorithms.

It is shown in [Conti13] that cache pollution attack is a realistic threat on NDN. The researchers have conducted experiments to confirm that the attacks previously demonstrated on very small topologies can extend on larger and more realistic networks with no additional effort. They point out that existing proactive countermeasures are ineffective against realistic adversaries. Also detecting and limiting the attack may prove to be a better strategy. Their simulations show that the lightweight detection technique provides accurate results. The technique can be applied to various topologies, and are independent from the distribution of the traffic routed by each node. Other possible strategies range from rate-limited traffic corresponding to malicious interests, to caching only content that would not significantly change the detection statistics.

In [Lauinger12], the authors aim to raise awareness of privacy attacks as an intrinsic and relevant issue in NDN architectures. They argue that the tradeoff between privacy and performance can be balanced at several layers of abstraction:

- Whether certain protocol features should be allowed
- At what aggregation level caches should be placed
- What content may be cached

Given an approach to classify objects according to their sensitivity, the most fine-grained one is to leave the major non-sensitive traffic unaffected and to prevent privacy-sensitive content from being cached. Privacy-sensitive contents are very likely be less popular, thus precluding them from caching not only improves privacy, but might increase the overall network efficiency as well. Because the privacy/caching issue is intrinsic in NDN architectures, there is an urgent need for privacy concepts that goes beyond the traditional â€œtunnelingâ€ approach. Current communication traces can be misused and exploited in so many ways that it is not realistic to expect users to correctly appreciate when they need to have protection mechanisms switched on.

Cache snooping is to probe whether certain data are store in the cache of a given router and relate such data to its consumers. [Ntuli12] propose an approach that detects cache snooping attempts targeted low-level routers. Their detecting algorithm takes input:

- the network graph, g
- the candidate selection function, f
- the trust function, t

The trust function is a mapping of trustworthiness between two connected nodes in the graph. A node satisfying f is defined as a candidate. A candidate that further satisfies t is called a snooper. When the algorithm initiates,it creates two empty sets: one set contains snoopers and the other one contains candidates. For each node in graph G, f is used to select candidates. The trust function t is called to determine snoopers from candidates. In function t, a candidate with computed trustworthiness less than the threshold k is regarded as a snooper. The output of the above procedure is the set of detected snoopers out of candidates. Such algorithm combines formal signatures with trust systems and pattern recognition to increase the level of confidence in snooper detection.

4. NDN Routing

As mentioned in NDN agenda, the research agenda of NDN routing can be split into the initial and the long-term deployment phase. The initial stage aims to extend the implementations of the intra-domain OSPF protocol and the inter-domain BGP routing protocol to enable immediate implementation. This allows the team to study two issues in multipath routing that will be informative to subsequent researches:

- preventing multi-path forwarding of Interest packets from inducing loops
- determining the optimal number and diversity of paths to maximize the probability and performance of data delivery
- minimizing computation, latency, and overhead

In long-term routing research, the team will develop native routing protocols tailored for NDN and focus on scalability. One of the protocols developed is NLSR, a link state protocol for NDN. Others have proposed a two-layer Intra-domain scheme for NDN.

From a domainâ€™s point of view, routing can be split into inter-domain routing and intra-domain routing. Inter-domain routing policies and schemes will be discussed in section 4.1. and specific intra-domain routing protocols will be covered in section 4.2.

4.1 Inter-Domain Routing Policies

Intra-domain routing using BGP is rather based on ISP policies than finding the least cost paths. Network operators design policies that affect route selection. These policies are implemented through tuning a set of knobs in BGP. NDN will also utilize a similar policy-based inter-ISP routing protocol. However, NDN enables finer granular policies by based routing on content names rather than hostsâ€™ locations. Therefore NDN creates more opportunities engineering traffic. [DiBenedetto11] explores possible routing policies in NDN. They have listed and described the knobs available to network operators and the possible settings. Table.1 summarizes those policy knobs [DiBenedetto11].

Table. 1 Summary of NDN Policy Knobs

Component	Name	Controls	Setting	Description
Control Plane	**Routing/RIB**	**Routes**	Not Selected	Route cannot be used to forward Interest Packets.
			Selected	Route may be used for forwarding Interest Packets.
			Selected and anounce	Route may be used for forwarding Interest Packets and may be announced to peer groups.
Content Store	**Cache Access**	**Interests**	Allow	Check interest against cache and proceed to PIT if no matches are found.
			Cache Only	Check interest against cache and drop if no matches are found.
			Deny	Drop interest without checking cache.
FIB	**FIB Usage**		Full Usage	New matching faces may be found and added to the existing face list.

			Limited Usage	No new faces may be added to the existing face list.

The discussions show that while multi-path routing may be considered one of NDNâ€™s greatest strengths, economic incentives could also encourage the system to favor fewer paths in order to reduce costs. Furthermore, economic incentives of content caching offer a number of new possibilities such as Cache Sharing between peers and Routing Rebates between customers and providers. The work also shows that policy can impact the PIT as well the traditional FIB and new cache.

4.2 Intra-Domain Routing Protocols

In order to provide name-based routing capability in NDN, [Wang12b] have extended OSPF to distribute name prefixes and calculate routes to name prefixes. The proposed OSPFN protocol is currently deployed in the NDN test bed. The goal is to develop a dynamic routing protocol for NDN to support the above functionality. As mentioned before, it is desirable for the long term to design a brand new protocol over the NDN architecture directly, naming routers and messages without using IP addresses and employing Interest/Data messages to exchange routing information. However, because there is an urgent need to support all NDN research areas to use the NDN test bed for prototyping and evaluation, an implemented routing protocol is of top priority. Therefore the authors decided to extend the existing OSPF because it is widely used in the Internet and it has high-quality open-source implementations.

OSPFN version 1.0 is name-based, runs over IP and supports only single-path routing. In version 2.0, configured multipath support is then added. OSPFN uses Opaque Link State Advertisements (OLSA) to announce name prefixes while ensuring backward compatibility. It supports name prefix advertisement from multiple sites and since OSPF provides only a single best path to destination, configured multipath is added to specify the links to use when the best route fails to bring back data. Although OSPFN does not support full-fledged dynamic multipath routing capability, the configured multipath has already helped a lot to understand the forwarding behavior pattern of the current CCND implementation. OSPFN is deployed at all the ten institutions participating in the NDN test bed.

While OSPFN can perform the very basic operations of NDN routing, it has significant limitations [Hoque13]. OSPFN still uses IP addresses as router IDs, relies on GRE tunnels to cross legacy networks, and computes only single best next-hops for each name prefix. Their experience from OSPFN deployment indicates that managing IP addresses and tunnels are the two major operational problems, and the limited multipath support hinders NDNâ€™s effectiveness.

The researchers then present a design of the Named-data Link State Routing protocol (NLSR) [Hoque13], a customized routing protocol for NDN. NLSR propagates reachability to name prefixes instead of IP prefixes and differs from IP-based link state protocols in two fundamental ways. First, NLSR uses Interest/Data packets to advertise routing updates, directly benefiting from NDNâ€™s data authenticity. Second, NLSR generates a list of forwarding options with ranks for each name prefix in order to facilitate NDNâ€™s adaptive forwarding strategies. Third, NLSR offers more efficient update dissemination, built-in update authentication, and native support of multipath forwarding.

The shift from OSPFN to NLSR shows the routing protocol evolution in NDN research. There are other researchers proposing routing schemes targeting at NDN. Their works are introduced below.

[Dai12] propose a two-layer routing protocol for NDN. The underlying layer maintains the topology information of the NDN network domain and calculates the shortest-path tree rooted at each node and thus is called Topology Maintaining (TM) layer. The TM layer provides the shortest paths information as a service to the upper layer: Prefix Announcing (PA) layer. The PA layer runs on TM layer and publishes the content that the router wants to serve by sending out announcements. The announcements are forwarded to all the other nodes via the single source shortest-path tree rooted at this router provided by TM layer. At this layer, routers build their own FIBs based on received announcements. The two-layer architecture is shown in Figure 7 [Dai12].

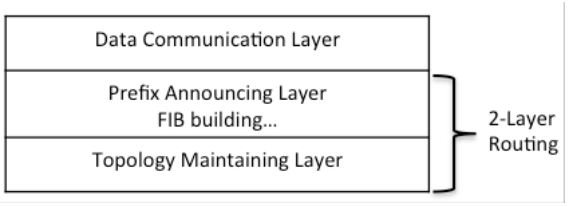


Figure 7. Layered Routing Hierarchy

[Torres12] propose a Controller-based Routing Scheme (CRoS) for NDN. CRoS defines a special network element called controller who is responsible for the named data location storage and routing. The controllers learn the topology in the bootstrap phase and compute routes to all the routers. In this phase, the router-controller routes are installed in routers while routes to named data are not. After the bootstrap phase, new named data is registered in the controllers that store the named dataâ€™s location. Then a router can request the controllers for installation of a new route to an unknown prefix. Since all named data locations are now registered in the controllers, they can calculate routes to any valid named data.

CRoS runs on top of the NDN and uses only NDN packets. Therefore it preserves NDN features such as congestion control, network failure detection and path diversity. Nonetheless, CRoS uses special interest packets with semantically meaningful names to reduce control overhead. To avoid the explosion of named data location storage in the controllers, Distributed Hash Tables (DHT) are used to balanced the storage between existing controllers and new ones can be added with minimal impact.

5. Summary

In this paper, an overview of the Named Data Networking project is first introduced. NDNâ€™s architecture design principles and building blocks are described in comparison with the current IP-based network. The following research agenda covers important issues of high study priority. Among these topics there are NDN caching and routing, which are covered respectively.

Caching schemes are first discussed and several proposals are subsequently covered. Researchers proposing the effective caching scheme compare three caching algorithms and concludes that the Bridging combines the advantages of both Bottom Up and Top Down and the simulation result show such caching scheme based on Bridging outperform LCE significantly. Other researchers design data structures for NDN caching. Cache management schemes are proposed to improve cache hit ratio and reduce data access time. Many other works address the privacy and security concerns raised by NDN caching. Potential privacy attacks based on cache such as cache snooping and cache pollutions attacks are discussed and countermeasures against these attacks are covered.

On the issue of NDN routing, firstly, a summary of the tunable knobs for the policymaking is presented in the discussion of NDN inter-domain routing. These knobs spread across NDNâ€™s control plane, Content Store and FIB. Then the evolution of intra-domain routing protocols is described. An extension of OSPF is adopted to meet the urgent need of a running routing protocol for the test beds at the initial deployment phase. Then the NLSR is development to achieve the long-term goal for routing scalability and is more customized

for NDN. Other researchers have proposed routing solutions such as 2-layered routing and controller-based routing schemes. These proposals are also great contributions to the NDN routing research field.

6. List of Acronyms

The acronyms are listed alphabetically.

Acronym	Standing For
BGP	Border Gateway Protocol
CCN	Content-Centric Network
CCND	Content-Centric Network Daemon
CRoS	Controller-based Routing Scheme
CS	Content-Centric Network
DHT	Distributed Hash Table
FIB	Forwarding Interest Base
LCE	Leaving Copies Everywhere
ISP	Internet Service Provider
NLSR	Named Data Link State Routing Protocol
OLSA	Opaque Link State Advertisements
OSPF	Open Shortest Path First
OSPFN	OSPF for Named Data
P2P	Point-to-Point
NLSR	Named Data Link State Routing Protocol
PA	Prefix Announcing
PID	(Packet | Data) tuple
PIT	Pending Interest Table
TM	Topology Maintaining

7. References

References are indexed in alphabetical order.

[Acs13] Acs, G., M. Conti, P. Gasti, C. Ghali and G. Tsudik (2013). Cache Privacy in Named-Data Networking, ICDCS. URL: http://camera.crysys.hit.bme.hu/~acs/publications/AcsCGGT13icdcs.pdf

[Conti13] Conti, M., Gasti, P., & Teoli, M. (2013). A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. Computer Networks, 57(16), 3178-3191. URL:http://www.sciencedirect.com/science/article/pii/S1389128613002818

[Dai12] Huichen Dai; Jianyuan Lu; Yi Wang; Bin Liu, "A two-layer intra-domain routing scheme for named data networking," Global Communications Conference (GLOBECOM), 2012 IEEE , vol., no., pp.2815,2820, 3-7 Dec. 2012. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&rnumber=6503543&snumber=6503052

[DiBenedetto11] Steven DiBenedetto, Christos Papadopoulos, and Daniel Massey. 2011. Routing policies in named data networking. In Proceedings of the ACM SIGCOMM workshop on Information-centric networking (ICN '11). ACM, New York, NY, USA, 38-43. URL:http://doi.acm.org/10.1145/2018584.2018595

[Hoque13] A K M Mahmudul Hoque, Syed Obaid Amin, Adam Alyyan, Beichuan Zhang, Lixia Zhang, and Lan Wang. 2013. NLSR: named-data link state routing protocol. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking (ICN '13). ACM, New York, NY, USA, 15-20. URL:http://doi.acm.org/10.1145/2491224.2491231

[Lauinger12] Tobias Lauinger, Nikolaos Laoutaris, Pablo Rodriguez, Thorsten Strufe, Ernst Biersack, and Engin Kirda. 2012. Privacy risks in named data networking: what is the cost of performance? SIGCOMM Comput. Commun. Rev. 42, 5 (September 2012), 54-57. URL:http://doi.acm.org/10.1145/2378956.2378966

[Li12a] Jun Li; Hao Wu; Bin Liu; Jianyuan Lu, "Effective Caching Schemes for Minimizing Inter-ISP Traffic in Named Data Networking," Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on , vol., no., pp.580,587, 17-19 Dec. 2012 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&rnumber=6414460&snumber=6413550

[Li12b] Jun Li, Hao Wu, Bin Liu, Jianyuan Lu, Yi Wang, Xin Wang, YanYong Zhang, and Lijun Dong. 2012. Popularity-driven coordinated caching in named data networking. In Proceedings of the eighth ACM/IEEE symposium on Architectures for networking and communications systems (ANCS '12). ACM, New York, NY, USA, 15-26. URL:http://doi.acm.org/10.1145/2396556.2396561

[Ntuli12] Ntuli, N. and S. Han (2012). Detecting router cache snooping in Named Data Networking. ICT Convergence (ICTC), 2012 International Conference on, IEEE. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&rnumber=6387155&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6387155

[Torres12] J. Torres, L. Ferraz, and O. Duarte. Controller-based routing scheme for Named Data Network. Technical report, Electrical Engineering Program, COPPE/UFRJ, December 2012. URL:http://www.gta.ufrj.br/ftp/gta/TechReports/TFD12.pdf

[Wang12a] Wang, H., Z. Chen, F. Xie and F. Han (2012). A Data Structure for Content Cache Management in Content-Centric Networking. 2012 Third International Conference on Networking and Distributed Computing, Oct. 2012, pp.11-15 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&rnumber=6386698&snumber=6386572

[Wang12b] Wang, L., A. Hoque, C. Yi, A. Alyyan and B. Zhang (2012). "OSPFN: An OSPF based routing protocol for Named Data Networking." University of Memphis and University of Arizona, Tech. Rep. URL:http://www.named-data.net/techreport/TR003-OSPFN.pdf

[Zhang10] Zhang, L. et al., "Named Data Networking (NDN) Project." Technical Report NDN-0001, NDN, 2010. URL:http://www.named-data.net/ndn-proj.pdf

---

Last Modified: December 10, 2013

This and other papers on latest advances in computer networking are available on line at http://www.cse.wustl.edu/~jain/cse570-13/index.html

Back to Raj Jain's Home Page