Internet Research Task Force (IRTF)
Request for Comments: 7927
Category: Informational
ISSN: 2070-1721

D. Kutscher, Ed.
NEC
S. Eum
Osaka University
K. Pentikousis
Travelping
I. Psaras
UCL
D. Corujo
Universidade de Aveiro
D. Saucez
INRIA
T. Schmidt
HAW Hamburg
M. Waehlisch
FU Berlin
July 2016

Information-Centric Networking (ICN) Research Challenges

Исследование ориентированных на информацию сетей

Аннотация

В этом документе описаны требующие исследования вопросы ориентированных, на информацию сетей (Information-Centric Networking или ICN), подхода к развитию инфраструктуры Internet для прямой поддержки распространения информации путём введения данных с уникальными именами в качестве базового принципа Internet. Данные становятся независимыми от их местоположения, приложений, хранилищ и способов доставки, что обеспечит или улучшит множество желаемых функций, таких как безопасность, мобильность пользователей, групповая передача и кэширование в сети. Механизмы для решения этих задач являются темой ведущихся исследований в рамках IRTF и других местах. Этот документ описывает текущие задачи исследования ICN, включая именование, безопасность, маршрутизацию, расширяемость систем, управление мобильностью, беспроводные сети, транспортные службы, кэширование в сети и управление сетями.

Документ является результатом работы исследовательской группы IRTF ICNRG (Information-Centric Networking Research Group).

Статус документа

Этот документ не задаёт стандарта Internet (Standards Track) и публикуется с информационными целями.

Документ является результатом работы IRTF[1]. IRTF публикует результаты связанных Internet исследований и разработок. Эти результаты могут не подходить для развёртывания. Данный документ представляет согласованное мнение исследовательской группы Information-Centric Networking в составе IRTF. Документы, одобренные для публикации IRSG не являются кандидатами в какие-либо стандарты Internet (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7927.

Оглавление

1. Введение....2
2. Проблемы ориентированного на хосты взаимодействия....2
3. Терминология и концепции ICN....3
   3.1. Термины....3
   3.2. Концепции....3
4. Исследовательские задачи ICN....4
   4.1. Именование, целостность данных и подлинность источника данных....4
   4.2. Безопасность....5

[1]Internet Research Task Force - комиссия по исследованиям Internet.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

4.2.1. Целостность данных и проверка подлинности источника....5
4.2.2. Привязка NDO к объектам реального мира....5
4.2.3. Контроль доступа и проверка полномочий....5
4.2.4. Шифрование....6
4.2.5. Объединение и фильтрация трафика....6
4.2.6. Перезагрузка состояния....6
4.2.7. Доставка объектов данных из реплик....6
4.2.8. Криптографическая стойкость....6
4.2.9. База данных маршрутизации и пересылки....7
4.3. Расширяемость маршрутизации и системы распознавания....7
4.3.1. Маршрутизация по именам....7
4.3.2. Маршрутизация с поиском по именам....7
4.3.3. Гибридная маршрутизация....7
4.4. Поддержка мобильности....8
4.5. Беспроводные сети....9
4.6. Контроль скорости и перегрузок....9
4.7. Кэширование в сети....10
4.7.1. Размещение кэша....10
4.7.2. Распространение содержимого по кэшам....10
4.7.3. Маршрутизация по запросам к кэшу....11
4.7.4. Обнаружение несвежести кэшированных NDO....11
4.7.5. Совместное использование кэша несколькими приложениями....11
4.8. Управление сетью....11
4.9. Применение ICN....12
4.9.1. Web-приложения....12
4.9.2. Видеопотоки и загрузка....13
4.9.3. Internet вещей....13
5. Вопросы безопасности....13
6. Литература....13
Благодарности....15
Адреса авторов....15

1. Введение

Информационно-ориентированная сеть (ICN) - это подход к развитию инфраструктуры Internet для прямой поддержки доступа к именованным объектам данных (Named Data Object тлт NDO) в качестве сетевой службы первого порядка. Объекты данных становятся независимыми от местоположения, приложений, хранилищ и способов доставки, позволяя организовать недорогое и повсеместное кэширование и репликацию в сети. Ожидаемыми преимуществами являются рост эффективности, безопасности и расширяемости по отношению к требованиям пропускной способности, а также повышение отказоустойчивости в сложных сценариях взаимодействия.

Концепции ICN можно реализовать путём переоснащения стека протоколов - доступ к данным по именам можно реализовать на основе имеющейся инфраструктуры IP, например, разрешая именованные структуры данных, повсеместное кэширование и соответствующие транспортные службы или же такой доступ можно рассматривать как технологии межсетевого взаимодействия на уровне пакетов, что может привести к фундаментальным изменениям маршрутизации и пересылки в Internet. Таким образом, ICN может развивать архитектуру Internet в направлении модели сети, основанной на именованных данных с разными свойствами и разными услугами.

В этом документе представлены направления исследования ICN, которые нужно реализовать для достижения заявленных целей. Эти исследовательские задачи можно рассматривать с технической точки зрения, хотя деловые взаимоотношения между игроками Internet также будут влиять на исследования. Однако вопросы бизнеса оставлены для отдельного документа. Целью этого документа являются технические вопросы и соответствующие текущие подходы, а также определение требований, которые нужно рассматривать в будущих исследованиях.

Этот документ рассмотрен и широко обсуждался в течение почти двух лет большинством членов ICNRG (число более 100). Документ выражает согласованное мнение ICNRG, что описанные здесь исследовательские задачи следует опубликовать в потоке IRTF серии документов RFC. Данный документ не задаёт какого-либо стандарта.

2. Проблемы ориентированного на хосты взаимодействия

Наилучшим современным опытом управления упомянутым выше ростом в терминах объёма данных и числа устройств является рост инвестиций в инфраструктуру, реализация наложений на прикладном уровне с кэшированием содержимого, например сети распределения содержимого (Content Distribution Network или CDN) и одноранговые (Peer-to-Peer или P2P) приложения, обеспечивающие доступ к данным независимо от местоположения и оптимизацию доставки. В принципе, такие платформы предоставляют модель обслуживания с доступом к именованным объектам данных (named data object или NDO), например, репликацию web-ресурсов в ЦОД вместо модели доставки пакетов от хоста к хосту.

Однако по причине наличия такой функциональности только в наложенных системах, весь потенциал платформ распределения содержимого не может быть использован, поскольку сеть не знает о запросах и передаче данных. Влияние этого перечислено ниже.

- Трафик данных обычно проходит по неоптимальным путям, поскольку он маршрутизируется в зависимости от топологии наложения, а не топологии на уровне Internet.
- Возможности сети, такие как групповая и широковещательная передача, используются недостаточно или не применяются совсем. В результате запросы и доставка для одного и того же объекта выполняются много раз.
- Для наложений обычно требуется значительная инфраструктурная поддержка, например, порталы аутентификации, хранилища содержимого и серверы приложений, что зачастую делает невозможной организацию прямого локального взаимодействия.

- Уровень пересылки не может взаимодействовать с функциями транспортного уровня, поэтому иногда такие полезные функции как локальный повтор передачи и локальный контроль скорости приходится реализовать с помощью посредников TCP или иных промежуточных устройств.

- Сегодня для проверки происхождения применяется аутентификация хостов, поэтому даже при наличии локально кэшированных копий обычно проверка их подлинности непроста.

- Многие (если не все) приложения применяют свой подход к кэшированию, репликации, доставке и проверке подлинности, хотя все они используют похожие модели доступа к именованным объектам в сети.

Ориентированные на хосты коммуникационные системы ограничивают приложения передачей данных лишь между конечными хостами. Именование данных напрямую обеспечивает «ловушку» для приложений, чтобы использовать и естественным способом поддерживать групповое взаимодействие и повсеместную информационную систему, не ограничиваемую адресами конечных хостов.

3. Терминология и концепции ICN

3.1. Термины

Information-Centric Networking (ICN) - ориентированная на информацию сеть

Концепция сетевого взаимодействия, обеспечивающая доступ к именованным объектам данных как сервис первого уровня. См. 3.2. Концепции.

Named Data Object (NDO) - именованный объект данных

Адресуемый блок данных в сети ICN, который можно представить как набор байтов или часть информации. В ICN каждый объект данных имеет имя и обычно существуют механизмы для защиты (и проверки) привязки имени к объекту. В разных подходах ICN применяются разные концепции отображения NDO на отдельные элементы передачи, например, блоки (chunk) или сегменты. Иногда наиболее мелким элементом являются сами NDO. В контексте этого документа NDO - это любой именованный объект, который можно запросить через сеть, и дополнительное дробление NDO на части не рассматривается. Термины NDO и «объект данных» в этом документе взаимозаменяемы.

Requestor - запрашивающий, заявитель

Элемент (сущность) в сети ICN, передающий в сеть запрос для именованного объекта данных.

Publisher - издатель

Элемент (сущность) в сети ICN, публикующий NDO в сети так, что соответствующие запросы могут попадать к издателю. Издатель может не совпадать с исходным создателем данных, например, издатель может предоставлять услуги хостинга NDO от имени их реальных создателей (владельцев).

3.2. Концепции

Фундаментальным свойством ICN является предоставление доступа к именованным данным в качестве сетевой услуги первого уровня, т. е. сеть способна запрашивать именованные данные естественным способом. Это означает, что узлы сети могут получать запросы для именованных объектов и действовать подобающим образом, например, пересылать запрос на подходящий следующий интервал (next hop). Поэтому сеть обрабатывает запросы для именованных объектов данных естественным способом. Каждому узлу сети на пути разрешено принимать решения о пересылке, кэшировании объектов и т. п. Это позволяет сети пересылать такие запросы по оптимальному пути, реализуя на каждом узле наилучшую технологию передачи (например, групповую или широковещательную передачу в беспроводной сети для предотвращения отправки дубликатов запросов и откликов).

В ICN имеется набор базовых концепций и требований к узлам, выходящих за пределы этой базовой модели. Именование объектов данных является ключевой концепцией. В общем случае имена в ICN не представляют ни узлы сети, ни интерфейсы - они представляют NDO независимо от их размещения.

Имена играют ключевую роль в решениях о пересылке и служат для сопоставления запросов с откликами - чтобы обеспечить лучшую поддержку доступных копий NDO независимо от места их размещения, важна способность убедиться, что отклик действительно доставляет биты, соответствующие исходному запросу именованных данных.

Проверка привязки имени к содержимому является фундаментальным средством защиты в ICN и это часто обеспечивается организацией проверяемой привязки между именованным объектом и фактическим объектом или элементом (сущностью), создавшим этот объект. ICN может поддерживать другие услуги защиты, такие как проверка происхождения и шифрования, в зависимости от деталей схем именования, моделей объектов и допущений об инфраструктурной поддержке. Услуги защиты, такие как привязка имён к содержимому, доступны любому узлу, а не только фактическим заявителям. Это свойство важно для обеспечения входным шлюзам возможности проверить подлинность объекта для предотвращения DoS-атак (отказ в обслуживании.

На основе этих фундаментальных свойств можно повсеместно применять сетевые хранилища - каждый узел ICN может кэшировать объекты данных и отвечать на запросы таких объектов, при этом не требуется проверять подлинность самого узла, поскольку можно проверить привязку имени к содержимому. Повсеместные хранилища в сети можно применять с разными целями, например для общего пользования, когда одна и та же копия объекта может быть доставлена множеству пользователей (узлов), как в современных кэширующих прокси и CDN[1]. Они могут также служить для повышения отказоустойчивости (и производительности), позволяя сети отвечать на запросы данными из локального кэша, а не от исходного сервера. В случае сбоя (сообщение не доставлено) узел может повторно передать запрос и ответ будет возвращён из имеющегося на пути кэша, т. е. с другой стороны повреждённого канала. Сама сеть будет способна повторять локалюные передачи, что позволит сократить время кругового обхода (round-trip) и разгрузить исходные серверы и другие части сети.

ICN может извлекать сегменты NDO из разных источников, поэтому лишь запрашивающий может проверить полноту извлечения, т. е. запрашивающая сторона обычно контролирует извлечение NDO или отдельных сегментов. По этой причине транспортные протоколы ICN обычно базируются на механизмах с контролируемой доставкой - запрашивающий может контролировать скорость передачи, регулируя скорость отправки запросов (в предположении, что каждый отклик вызван получением запроса). Повторная передача может обеспечиваться повтором запросов,

[1]Content Delivery Network. *Прим. перев.*

например, по тайм-ауту. Поскольку объекты могут быть реплицированы, их передача и транспортные сессии не обязаны иметь сквозную семантику, ответ на запрос можно получить из кэша и узел может выбрать для конкретного запроса получателя в одном или нескольких интервалах (next-hop) в зависимости от конфигурации, наблюдаемой производительности и других критериев.

Такая модель управляемого получателем взаимодействия может открывать новые модели связи между сетями и бизнеса. Запрос именованного объекта может быть привязан к интересам запрашивающего (или его сети) в данных от другого партнёра, что позволяет предложить соответствующие модели партнерских соглашений и оплаты услуг.

4. Исследовательские задачи ICN

4.1. Именование, целостность данных и подлинность источника данных

Именование данных важно для ICN, как именование хостов для сегодняшней сети Internet. Фундаментальным требованием ICN является уникальность имён отдельных NDO, поскольку эти имена служат для идентификации объектов независимо от места их расположения или контейнера. Кроме того, возможность кэширования NDO в любом месте не позволяет больше доверять источнику и требует обеспечения возможности проверять привязку объектов к именам (проверка привязки имени к данным), чтобы запрашивающий мог быть уверен в получении битов, соответствующих исходно запрошенному NDO (целостность данных). Проверка подлинности источника данных является другой службой защиты, которая может быть связана с именованием. Фактически это проверка того, что NDO действительно опубликован издателем, который может быть определён по префиксу имени.

Указанные выше функции необходимы для надёжной работы ориентированной на информацию сети, поскольку без них ни элементы сети, ни запрашивающие не могут считать объекты подлинными. Отсутствие доверия открывает возможность для ряда атак, включая DoS, путём внедрения подставного содержимого в сеть. Есть два разных способа применения имён и криптографии для обеспечения желаемых функций [ICNNAMING] [ICNSURVEY] и много разных способов поддержки пространства имён.

В литературе предложено две схемы именования для ICN - с иерархическим и плоским пространством имён. Например, в иерархической схеме может применяться структура, похожая на современные URI[1], где корнем иерархии служит префикс издателя. Такая иерархия позволяет агрегировать маршрутные данные, улучшая возможности расширения системы маршрутизации. В некоторых случаях имена являются удобными для людей, что позволяет пользователям набирать имена вручную, использовать имена многократно и в той или иной степени сопоставлять имена с намерениями пользователей.

Другой базовый тип схем именования позволяет проверять для объектов целостность связи объект-имя без использования инфраструктуры открытых ключей (Public Key Infrastructure или PKI) или иных сторонних систем обеспечения доверенных ключей. Это можно обеспечить, например, привязкой хэш-значения содержимого NDO к имени объекта. Хэш-значение можно встраивать напрямую в имя. Другим вариантом служит опосредованная привязка, где открытый ключ издателя встраивается в имя и подписывается хэш содержимого с помощью соответствующего секретного ключа. Получаемые в результате имена обычно не имеют иерархии, т. е. пространство имён является плоским, хотя имя может включать поле издателя для создания структуры, позволяющей агрегировать маршруты.

Имеется несколько компромиссных решений по именованию в ICN, влияющих на маршрутизацию и безопасность. Имена на основе хэш-значений непонятны человеку и не поддерживают иерархии. Однако они могут поддерживать некоторую структуру для агрегирования, например путём включения издателя в имя. В именах на основе хэша с опосредованной привязкой ключ издателя привязывается к имени NDO так, что при получении пользователем, например, триплета (данные, ключ, подпись), получатель может убедиться, что NDO создан владельцем пары ключей (открытый и секретный) и содержимое NDO не поменялось при передаче (целостность данных). Это можно сделать с помощью криптографического хэширования полученного ключа и имени NDO с последующим сравнением результата с полученным хэшем ключа. Затем ключ можно использовать для проверки подписи.

Проверку подлинности источника данных можно выполнить, проверяя криптографическую подпись с использованием криптографии с открытым ключом для имени и содержимого NDO. Чтобы удостовериться в целостности данных и подлинности источника при таком подходе нужна схема, похожая на PKI, которая позволит связать соответствующий открытый ключ с цепочкой доверия.

Темы для исследования, связанные с именованием, приведены ниже.

- Именование статических объектов данных можно реализовать путём включения хэш-значения объекта как части имени, чтобы издатель мог рассчитать хэш для имеющихся объектов данных, а запрашивающие и любые узлы ICN могли проверить привязку имени к содержимому повторным расчётом хэш-значения и сравнением его с именем или его частью. В [RFC6920] описан формат именования для этого случая.

- Именование динамических объектов относится к случаям, когда имя создаётся раньше объекта. Например, это может быть потоковое вещание, когда издатель хочет сделать поток доступным путём регистрации имён его блоков в сети. Одним из подходов для этого являются основанные на хэш-значениях имена с опосредованной привязкой, как указано выше.

- Защита приватности запрашивающей стороны может быть проблемой в ICN как прямое следствие парадигмы доступа к именованным объектам данных - если сеть может «видеть» запросы и отклики, она может записать историю запросов для сегментов сети или отдельных пользователей, что может быть нежелательно, особенно в случаях использования долгоживущих имён. Т. е. даже если имя само на раскрывает излишних сведений, это имя может позднее использоваться для извлечения соответствующих данных.

- Обновление и версии NDO могут вызвать проблемы, поскольку они могут противоречить фундаментальным допущениям ICN. Если NDO можно реплицировать и сохранить в сетевом кэше для последующего извлечения, имена должны быть долгоживущими и привязки имён к содержимому должны сохраняться, обновление объекта (т. е. изменение его содержимого без создания нового имени) становится невозможным. Управление

[1] Uniform Resource Identifier - унифицированный идентификатор ресурса. *Прим. перев.*

версиями является одним из возможных решений, но требует поддержки версий в схеме именования (и способа уведомления запрашивающих о версиях).

- Поддержка доступности также может быть связана с проблемами. В ICN принято базовое допущение о возможности повсеместного доступа к NDO, но возможны ситуации, когда доступ к объектам следует ограничить (например, предоставлять лишь определенным пользователям). Имеются различные подходы к решению этой задачи, такие как шифрование объектов (требуется распространение ключей и связанные с этим механизмы) или концепция области действия, например, по именам, которые могут использоваться и распознаваться лишь при определённых условиях.

4.2. Безопасность

Вопросы безопасности ICN активно исследуются. В этом разделе представлен обзор важных свойств защиты и соответствующих проблем, связанных с переходом к ориентированным на информацию сетям. Некоторые проблемы достаточно понятны и для ниж имеются решения (иногда несколько), а другие требуют активных исследований.

4.2.1. Целостность данных и проверка подлинности источника

Как отмечено в параграфе 4.1, проверка целостности данных является важной функцией в ICN, поскольку NDO можно получить не только от держателя исходного документа но и от разных точек кэширования. Поэтому конечные точки каналов для извлечения NDO не могут считаться доверенными и широко используемые решения, такие как защита на транспортном уровне (Transport Layer Security или TLS) [RFC5246], не могут обеспечить единого решения. Поскольку объекты данных могут быть подвергнуты вредоносным изменениям, в ICN следует обеспечивать механизм защиты для проверки целостности объектов данных и имеются разные способы решения этой задачи.

Эффективным решением для статических NDO является обеспечение привязки имени к содержимому путём хэширования NDO и использования хэш-значения как части имени объекта. В [RFC6920] описан механизм и формат представления алгоритма подписи (дайджеста), а также фактического дайджеста в имени (среди прочего).

Для динамических объектов, где желательно указание NDO по имени до создания объекта, часто применяется криптография с открытым ключом, т. е. подлинность каждого NDO проверяется с помощью подписи, создаваемой издателем объекта данных, чтобы любой потребитель мог проверить действительность объекта данных с помощью этой подписи. Однако для проверки подписи объекта потребитель должен знать открытый ключ подписавшей стороны.

Проверка подлинности источника данных, т. е. того, что NDO действительно создан издателем, требует защищённой привязки имени NDO к отождествлению издателя. Обычно это тоже реализуется с использованием криптографии с открытым ключом, т. е. получатель должен проверить цифровую подпись, являющуюся частью принятого сообщения.

Одной из задач исследований является механизм распространения открытых ключей издателей потребителям объектов данных. Для решения этой задачи имеется два основных подхода. Один подход основан на использовании сторонних средств, таких как иерархическая система открытых ключей (PKI) (см. [RFC5280]), а другой - в приспособлении основанной на хешировании схемы с опосредованной привязкой. Первый вариант, как ясно из названия, зависит от внешней системы распространения открытых ключей издателей между потребителями. В схеме на основе хэширования с опосредованной привязкой открытый ключ (или его хэш) служит частью имени и этого достаточно для проверки целостности данных.

Когда информация об источнике объекта данных недоступна другими способами, сам объект должен включать информацию, требуемую для определения издателя, например, сертификат, который можно проверить с помощью PKI. После проверки сертификата можно использовать открытый ключ для проверки подлинности подписанного объекта.

4.2.2. Привязка NDO к объектам реального мира

В дополнение к проверке подлинности NDO сохраняется важность привязки к объектам реального мира, например, к отождествлению издателя или объекту, чтобы запрашивающий мог убедиться, что полученный объект реально опубликован тем или иным источником.

Для основанных на хеш-значениях имён привязка к сущностям реального мира в действительности не создаётся, имена включают хэш NDO или открытого ключа, использованного для подписания NDO. Должна быть другая привязка к сущности реального мира, если это свойство запрошено.

Если имя объекта напрямую указывает имя издателя и это имя защищено сертификатом, связанным с цепочкой доверия в стиле PKI, имя объекта само может обеспечить привязку к сущности реального мира.

Привязки между NDO и элементами реального мира важны, но нет универсального способа создать их, поскольку в некоторых вариантах ICN они не являются естественными, присущими по природе.

4.2.3. Контроль доступа и проверка полномочий

Контроль доступа и проверка полномочий являются проблемой в ICN по причине отсутствия аутентификации на уровне клиент-сервер в базовой коммуникационной модели на основе именованных данных.

Все элементы ICN способны доставлять NDO по запросам благодаря функции кэширования в сети. В таких средах традиционные схемы контроля доступа на основе списков (Access Control List или ACL) плохо подходят поскольку широко распределённые элементы ICN должны поддерживать идентичные правила контроля доступа к NDO для каждого потребителя, что не представляется возможным из-за расчётных издержек и требований приватности. Имеется два взаимодополняющих подхода к решению этих проблем.

1. При раздельном подходе используется сторонняя служба контроля доступа, не зависимая от элементов ICN. В результате чёткого разделения элементы ICN освобождаются от расчётных издержек для определения доступности NDO потребителям, которые также могут защитить свою приватность с помощью независимого элемента проверки полномочий [ACCESS-CTL-DEL]. Проблемы такого подхода включают снижение задержки при проверке полномочий (взаимодействие со сторонней службой), актуальность и согласованность данных контроля доступа (при распространении списков управления доступом).

2. При интегрированном подходе контроль доступа выполняют элементы ICN. Этот механизм зачастую основан на шифровании содержимого и распространении ключей [ENCRYPTION-AC]. Как отмечено ранее, этот подход сопряжён с непомерно высокими издержками для элементов ICN из-за процесса проверки ключа. Хотя распространение ключей само по себе связано со сложностями, этот подход выгоден тем, что NDO можно извлекать без помощи внешних средств контроля доступа. Проблемы этого подхода перечислены ниже.

    1. Своевременное применение механизма контроля для динамических NDO в сетевых кэшах.
    2. Предоставление потребителям различных уровней доступа к отдельным NDO расширяемым способом.
    3. Поддержка отзыва ключей и похожих функций управления PKI.

4.2.4. Шифрование

В ICN объекты NDO могут шифроваться для реализации контроля доступа (только потребители, имеющие соответствующий ключ расшифровки могут получить доступ к содержимому) или приватности (тот же подход). Распространение и поддержка соответствующих ключей, а также предоставление применимых интерфейсов для приложений и пользователей являются проблемами и их исследование продолжается.

В принципе проблемы похожи на возникающие при широковещательном и групповом распространении содержимого (комбинация симметричного и асимметричного шифрования) и их изучение продолжается [NDN-CTL-SHARING].

4.2.5. Объединение и фильтрация трафика

Одно запросное сообщение для извлечения объекта данных может фактически объединять запросы от нескольких потребителей. Такое объединение запросов снижает суммарный трафик, но усложняет фильтрацию на уровне запрашивающих. Проблема в этом случае заключается в предоставлении механизма, который позволит объединять запросы и фильтровать их на уровне потребителя. Возможным решением является указание набора запрашивающих в объединённом запросе так, чтобы отклик мог указывать подмножество запрашивающих, которым разрешён доступ к объекту данных. Однако это решение требует взаимодействия с другими узлами сети и не пригодно для кэширования. Другим возможным решением является шифрование объектов данных и обеспечение возможности их расшифровки лишь уполномоченным потребителям. Это решение не препятствует кэшированию и не требует взаимодействия с сетью, однако оно предполагает механизм генерации групповых ключей (например, могут применяться разные секретные ключи для расшифровки одного и того же зашифрованного объекта данных) [CHAUM].

4.2.6. Перезагрузка состояния

Решения ICN использующие состояния промежуточных устройств для маршрутизации или пересылки запросов (например, CCN[1] [CCN]) подвержены атакам с отказом в обслуживании из-за перезагрузки или смены внутреннего состояния маршрутизатора (например, interest flooding - лавина интересов [BACKSCATTER]). Кроме того, пересылка с учётом состояния может открыть возможность организации атак, таких как истощение ресурсов или комплексные атаки на инфраструктуру маршрутизации. Задача состоит в том, чтобы подготовить маршрутизаторы и создать внутреннее состояние так, чтобы снизить чувствительность к атакам. Проблема усложняется, если протокол не предоставляет сведений об источнике сообщений. Без указания источника сложно отличить обычные (интенсивные) обращения к инфраструктуре от её злонамеренного использования.

4.2.7. Доставка объектов данных из реплик

Базовым свойством решений ICN является репликация данных и хранилища внутри сети. Доставка кэшированных реплик отвязывает потребление содержимого от источников данных, что ведёт к потере контроля (1) за доступом к содержимому и (2) распространением содержимого. В широко распространённой децентрализованной среде, такой как Internet, это вызывает несколько проблем.

Одна группа проблем связана с контролем доступа, без которого издатель теряет средства учёта и наблюдения за потреблением содержимого, ограничением сферы доступа, а также контроля числа копий его данных в сети, а также лишается возможности надёжно отозвать публикацию. Любой несогласованный или несинхронизированный кэш данных может помешать политике эффективного управления содержимым.

Другая группа проблем возникает из-за возможности усиления трафика в несвязанной среде. Решения ICN, пытающиеся параллельно получить содержимое из нескольких реплик или использовать несвязанные состояния маршрутизации в сети, а также распределенные злоумышленники могут одновременно инициировать передачу содержимого из нескольких реплик в направлении одного получателя (например, инициированная перегрузка - initiated overloads или блокада blockades [BACKSCATTER]). Методы смягчения таких угроз требуют строгих проверок пересылки, которым нужно согласование с процедурами кэширования (в пути или вне его).

4.2.8. Криптографическая стойкость

Издатели подписывают содержимое для обеспечения целостности данных и обеспечения возможности проверки подлинности объекта данных. Это фундаментальное требование ICN обусловлено распределённым кэшированием. Издатели создающие много подписей для содержимого с продолжительным действием дают время и данные атакующим для взлома криптографических свидетельств. Подписывание большого объёма данных упрощает распространённые атаки с попытками взлома ключа издателя. На основе наблюдений отмечен ряд направлений для исследования.

- В какой степени модель публикации содержимого конфликтует с криптографическими ограничениями?
- Как можно добиться незаметного повторного подписания без внесения дополнительных криптографических уязвимостей и издержек на управления ключами?

В общем случае реализации ICN следует разрабатывать с учётом рекомендаций [RFC7696] особенно в части гибкости криптоалгоритма, например, [RFC6920] задаёт схему именования для имён на основе хэширования, которая была разработана для поддержки гибкости алгоритмов.

[1] Content-Centric Networking - ориентированная на соединения сеть.

4.2.9. База данных маршрутизации и пересылки

В информационно-ориентированных сетях одним из векторов атак является увеличение размера таблиц маршрутизации и пересылки на узлах ICN, т. е. атак на расширяемость маршрутизации в сетях, основанных на маршрутизацию по именам. Это внутренняя проблема безопасности в ICN и возможные подходы к смягчению последствий таких атак включают сочетание проверки подлинности маршрутных данных с фильтрацией (например, максимальный уровень деагрегирования, когда это применимо, «черные списки» и т. п.).

4.3. Расширяемость маршрутизации и системы распознавания

Маршрутизация ICN - это процесс, находящий NDO на основе предоставленного запрашивающим имени. Маршрутизация ICN может включать три шага: (1) распознавание имени, (2) обнаружение и (3) доставку. Этап распознавания имени транслирует имя запрошенного NDO в его локатор. Этап обнаружения маршрутизирует запрос к объекту данных по его имени и локатору. На последнем этапе (доставка) объект маршрутизируется к запрашивающему. В зависимости от комбинации этих шагов схемы маршрутизации ICN можно разделить на категории маршрутизации по имени (Route-By-Name Routing или RBNR), поиска по имени (Lookup-By-Name Routing или LBNR) и гибридной маршрутизации (Hybrid Routing или HR), описанные в следующих параграфах.

4.3.1. Маршрутизация по именам

В RBNR не используется распознавание имён, поскольку имя NDO напрямую применяется для маршрутизации запроса к объекту данных. Поэтому маршрутная информация для каждого объекта данных поддерживается в таблице маршрутизации. Поскольку число таких объектов очень велико (10^{11} по оценкам 2007 г. [DONA], но может быть значительно больше, например от 10^{15} до 10^{22}), размер таблиц маршрутизации становится проблемой, поскольку он может быть пропорционален числу элементов данных, если не применяется механизмов агрегирования. С другой стороны, RBNR сокращает общую задержку и упрощает процесс маршрутизации за счёт отказа от распознавания. Для этапа доставки в RBNR нужен другой идентификатор (ID) хоста или местоположения, куда нужно пересылать запрошенные данные. В ином случае потребуется дополнительный механизм, такой как как маршрутизация по цепочке [BREADCRUMBS], где каждый запрос оставляет за собой след на пути его пересылки и отклик проходит обратно к запрашивающему по оставленному следу. Проблемы RBNR указаны ниже.

- Как объединить имена объектов данных для снижения числа маршрутных записей?
- Как пользователь может узнать имя, назначенное провайдером для агрегирования? Например, хотя мы называем свою работу «исследование проблем ICN», IRTF (провайдер) может поменять имя на «исследование проблем IETF/IRTF/ICN/» для агрегирования. Как в этом случае пользователь может узнать агрегированное имя для отыскания результатов исследования проблем ICN без процесса распознавания?
- Можно ли обеспечить расширяемую систему маршрутизации без механизма агрегирования, используя преимущества топологической структуры и распределенных копий? Например, будет ли компактная маршрутизация [COMPACT], случайный обход [RANDOM] или «жадная» маршрутизация [GREEDY] работать в масштабе Internet?
- Как встроить копии объектов данных в кэшах внутри сети в эту схему маршрутизации?
- Маршрутизация по следу предполагает симметричные пути для запросов и откликов в ICN. Некоторые конфигурации сетей и типы каналов препятствуют такой симметрии, поэтому будут возникать проблемы при подключении таких сетей к инфраструктуре с маршрутизацией по следу. Например, некоторые стратегии пересылки в устойчивых к задержкам сетях (Delay-Tolerant Networking или DTN) [RFC4838] реализуют пересылку так, что нельзя предполагать прохождение откликов по тому же пути, что служил для запроса.

4.3.2. Маршрутизация с поиском по именам

В LBNR сначала применяется распознавание имён для трансляции имени запрошенного объекта в его локатор, затем выполняется этап обнаружения на основе этого локатора. Поскольку локаторами могут служить адреса IP, этап обнаружения может зависеть от текущей инфраструктуры IP. Этап доставки можно реализовать подобно маршрутизации IP. Локатор запрашивающего включается в сообщение с запросом и запрошенные данные возвращаются по этому локатору. Экземпляром LBNR является [MDHT]. Проблемы LBNR перечислены ниже.

- Как построить расширяемую систему распознавания, которая обеспечит:
  - быстрый поиск - отображение имени объекта данных на его локаторы (включая копии);
  - быстрое обновление - расположение объектов данных может меняться достаточно часто и одновременно может меняться местоположение множества объектов данных (например, в переносных системах).
- Как встроить копии объектов данных из сетевых кэшей в эту схему маршрутизации?

4.3.3. Гибридная маршрутизация

HR комбинирует RBNR и LBNR для получения выгоды от их преимуществ. Внутри административного домена, например, ISP, где вопросы расширяемости можно решить при планировании сети, можно применить RBNR для снижения общей задержки за счёт отказа от распознавания. Между доменами, имеющими свои префиксы (локатор) можно использовать LBNR. Например, запрос изначально включает имя NDO для операции RBNR и пересылается к кэшированной копии NDO или исходному серверу. Когда для запроса не удаётся найти запись с таблице маршрутизации, запускается распознавание имён для трансляции имени в локатор, который будет служить для последующей пересылки сообщения с запросом.

Проблемы HR указаны ниже.

- Как разработать расширяемую систему отображения, которая по имени NDO будет возвращать локатор целевого домена, чтобы инкапсулировать и переслать запрос пользователя в этот домен?
- Как защитить данные отображений, чтобы вредоносные маршрутизаторы не могли перехватить запрос путём связывания его локатор?

- Как поддерживать связку между именем и содержимым NDO для проверки происхождения и целостности при смене имени из-за полученного локатора?

4.4. Поддержка мобильности

Поддержка мобильности уже более двух десятилетий активно применяется в ориентированных на хосты коммуникациях. В частности в рамках IETF, начиная с [RFC2002], было стандартизовано множество расширений IP, направленных на «обеспечение прозрачной маршрутизации дейтаграмм IP для мобильных узлов в сети Internet» [RFC5944]. Говоря кратко, поддержка мобильности в сетях IP ориентирована на локаторы и опирается на концепцию привязок мобильности как основы для обеспечения постоянного подключения к мобильным узлам (см. [MMIN]). Другие органы стандартизации, такие как 3GPP, использовали аналогичные подходы на основе привязок. Трафик к мобильному узлу и от него должен проходить через привязку, обычно используя набор туннелей, что позволяет мобильному узлу сохранять доступность при смене точки подключения к сети.

Излишне говорить, что поддержка мобильности усложняет сеть IP, поскольку в архитектуру сети добавляются специализированные элементы. Это отражается в плоскости управления, которая передаёт связанные с мобильностью управляющие сообщения, организует и удаляет туннели и т. п. Хотя в IP мобильная связность является второстепенной задачей, в ICN она считается основной средой развёртывания. Большинство (если не все) предложений ICN учитывает мобильность изначально, хотя и с разным уровнем детализации в архитектуре и протоколах. Тем не менее, до сих пор не предложено решения с определенным ответом по части обслуживания мобильности в ICN с использованием естественных примитивов. Фактически мобильность рассматривается на основе конкретных решений ICN, т. е. нет единой парадигмы, похожей на туннели через привязки мобильности в ориентированных на хосты сетях, которую можно было бы применять в разных решениях ICN. Хотя широко распространённые архитектуры мобильных сетей обычно включают свои элементы сети и связанные с ними протоколы, они придерживаются той же линии (привязки) в части поддержки мобильности. Подход к разработке, основанный на привязках, преобладает и в литературе по ICN.

Однако развёртывание привязок мобильности и туннелирование вероятно не являются лучшим направлением для исследований в части мобильных сетей ICN. По сути этот подход не ориентирован на информацию и независимость от местоположения. Кроме того, как отмечено в [SEEN], текущие схемы поддержки мобильности привязывают извлечение информации не только к определённому сетевому шлюзу (например, домашнему агенту в Mobile IP), но и к корреспондентскому узлу по причине сквозной природы ориентированных на хосты коммуникаций. Однако при смене точки подключения извлечение информации из исходного узла-корреспондента может стать неоптимальным. Это было показано, например, в [MANI], где простой механизм, включающий обнаружение новых провайдеров извлечения для того же объекта данных, явно преобладает над туннельным подходом в стиле Mobile IP в части времени загрузки объекта. Проблема здесь заключается в том, чтобы извлечь выгоду из сведений о местоположении, упрощая использование примитивов ICN с естественной поддержкой групповой адресации и anycast.

В именовании и распознавании имён ICN, а также связанных с ними функциях защиты следует поддерживать мобильность естественными средствами. Например, в CCN [CCN] нет ограничений на маршрутизацию по связующему дереву (spanning tree), что позволяет использовать преимущества нескольких интерфейсов или приспосабливаться к изменениям, вызываемым быстрыми перемещениями (т. е. нет необходимости связывать адреса уровней 3 и 2). На деле мобильность клиентов можно упростить, разрешая запросам на новое содержимое приходить с разных интерфейсов или через недавно подключённых точек присоединения к сети. Однако когда перемещающийся узел является (единственным) источником содержимого, поддержка со стороны сети может усложниться, включая пересылку обновлений и перестройки кэшей. Примером является служба разговоров через сеть, такая как аудио- и видео-звонки через сеть между двумя сторонами. Требования в этом случае более строги когда нужна поддержка бесшовной мобильности, особенно по сравнению с распространением содержимого, которое можно буферизовать. Ещё одним параметром, на который следует обратить внимание, является влияние применения беспроводных интерфейсов на основе различных технологий, где производительность и условия на канале, могут меняться в широких пределах в зависимости от множества факторов.

В ориентированной на хосты сети механизмы поддержки мобильности обеспечивают оптимальную передачу обслуживания (handover) и бесшовный (в идеале) переход от одной точки присоединения к другой. Однако в ICN традиционное понимание «точки присоединения» уже не применимо, поскольку коммуникации больше не ограничиваются доступом к объектам данных по их местоположению. Поэтому «бесшовный переход» в ICN гарантирует, что получение содержимого продолжается без каких-либо заметных изменений с точки зрения получающего это содержимое приложения ICN. Кроме того, этот переход должен происходить параллельно с механизмами идентификации и доставки содержимого ICN, что позволяет такие сценарии, как подготовка доставки содержимого в целевой точке присоединения до передачи обслуживания (для сокращения помех при переключении канала). Эти аспекты мобильности могут также быть тесно связаны с аспектами управления сетью в части применения правил, управления каналами и другими параметрами, требуемыми для организации канала связи узла с сетью.

Задачи для исследований в масти поддержки мобильности в ICN указаны ниже.

- Как полностью использовать преимущества естественных примитивов ICN для поддержки мобильности?
- Как избавиться от необходимости привязок мобильности в сети, поддерживающей групповую и anycast-передачу, а также извлечение информации независимо от местоположения?
- Как механизмы извлечения содержимого могут взаимодействовать с операциями конкретных каналов, такими как нахождение каналов, доступных для определённого содержимого?
- Как предложить мобильность в качестве услуги, активизируемой лишь при необходимости (для узла, содержимого, условий)?
- Как координировать поддержку мобильности между узлом и сетью для оптимизации и применения правил?
- Как обеспечить поддержку мобильности без ограничения расширяемости в ICN?
- Как будет влиять на процесс распознавания имён быстрое изменение топологии в случае мобильности источника содержимого?

4.5. Беспроводные сети

Сегодня все беспроводные технологии радио-доступа L2 разрабатываются с учётом использования стека протоколов IP и сохранения этого в обозримом будущем. Фиксируя стек протоколов, разработчики могут достаточно просто решить целый ряд вопросов, включая обработку разговоров (например, голосовых вызовов), а не только трафика web, поддержку групповой передачи и т. д. С другой стороны, широковещание, присущее природе беспроводных коммуникаций, не используется в полной мере. Напротив, исследователи чаще сосредотачиваются на введении механизмов, которые предотвращают нарушение работы сети «широковещательными штормами». Вопрос применения широковещания для нужд ICN ещё предстоит тщательно исследовать.

Беспроводные сети часто, но не всегда, переплетаются с мобильностью. Фактически, измерения часто показывают, что многие пользователи часто подключаются к одной точке доступа Wi-Fi на длительное время. Показательным примером, часто упоминаемым в разных вариантах в литературе по ICN, служит доступ к хранилищу документов во время встреч и конференций. Например, на обычной встрече рабочей группы IETF секретарь делает заметки, которые выгружаются в центральное хранилище (Рисунок 1). Затем каждый участник встречи получает копию документа на своё устройство для локального использования, комментирования и обмена с отсутствующими на встрече коллегами. Отметим, что в этом примере нет мобильности узлов и не имеет значения, загружается ли документ с примечаниями один раз в конце сессии или обновляется в потоковом режиме, как обычно принято сегодня для совместной работы с документами (в облаке).

Рисунок 1. Совместное использование документа на встрече.

В этом случае мы видим, что одни и те же биты объекта данных (заметки к встрече) должны пройти через беспроводную среду по меньшей мере N+1 раз, где N - число участников встречи, получающих копию. По сути, широковещательная среда втиснута в N+1 индивидуальный виртуальный канал. Можно возразить, что локальная беспроводная связь недорога, но в данном примере это не является критическим фактором. Фактический обмен информацией тратит впустую доступную пропускную способность сети N раз независимо от спектральной эффективности (или экономики) базовой беспроводной технологии. Эти потери являются прямым результатом переноса парадигмы удалённого доступа кабельных сетей на беспроводные, независимо от возможностей последней.

Ясно, что подход ICN, не учитывающий беспроводную природу интерфейсов, будет использовать такой же объем ресурсов, как в ориентированной на хосты парадигме. Сетевое кэширование в беспроводной точке доступа может снизить объем данных, передаваемых по обратному (backhaul) каналу, но, если использование беспроводной среды не изменить, NDO по-прежнему будет передаваться через беспроводную среду N+1 раз. Интеллектуальные стратегии кэширования, кооперация размещения реплик и т. п. просто не могут изменить это. С другой стороны, работа интерфейса в режиме захвата (promiscuous) и кэширование с учётом обстоятельств (opportunistic) в приведённом примере повысят эффективность использования беспроводной среды.

Можно утверждать, что при разработке новых технологий беспроводного доступа с учётом ориентированного на информацию уровня L3 многие из привычных для архитектуры «всё по IP» решений больше не будут работать.

Хотя это явно выходит за рамки документа, ниже указано несколько направлений исследования, которые могут быть интересны широкому кругу.

- Можно ли использовать беспроводные ресурсы в ориентированной на информацию парадигме более экономно, чем в современных беспроводных сетях «всё по IP»?
- Как в контексте беспроводного доступа можно использовать широковещательную природу среды для информационно-ориентированной сети?
- Даст ли стек протоколов ориентированной на беспроводную среду ICN существенный рост производительности? Насколько он будет отличаться от стека протоколов ориентированной на кабели ICN?
- Можно ли за счёт смены сетевой парадигмы на ICN на практике повысить спектральную эффективность (бит/с/Гц) беспроводной сети сверх доступной для ориентированного на хосты подхода? Как это повлияет на энергопотребление?
- Повысит ли работа интерфейса в режиме захвата вместе с кэшированием с учётом обстоятельств производительность сети ICN и насколько, если это возможно?
- Как можно поддержать разговорные службы не менее эффективно, чем в современных беспроводных сетях?
- Каковы преимущества сочетания ICN с сетевым кодированием в беспроводных сетях?
- Как в будущих сетях совместить естественным способом MIMO (Multiple-Input Multiple-Output) и CoMP (Coordinated Multipoint Transmission) с примитивами ICN?

4.6. Контроль скорости и перегрузок

Описанная выше модель ICN с управлением от получателя открывает новые возможности для разработки транспортных протоколов, поскольку не полагается лишь на сквозное взаимодействие между запрашивающим и отправителем. Запрошенный объект данных может быть доступен во множестве мест сети. В результате узел может

принять решение об использовании нескольких источников, например параллельной передачи нескольких запросов для одного NDO или переключения источников (или next hop) с подходящим планированием для серии запросов.

В этой модели запрашивающая сторона контролирует скорость передачи данных, регулируя отправку запросов, а затем выбирая источник или следующий интервал (next-hop). Конкретные проблемы зависят от подхода ICN, но общие проблемы для управляемых получателем транспортных протоколов (или механизмов, поскольку выделенный протокол может не требоваться) включают контроль потока и перегрузок, беспристрастность, загрузку сети, стабильность (скорости передачи при стабильных условиях) и т. п. В [HRICP] и [CONTUG] описаны протоколы управления передачей запросов и связанные с этим проблемы проектирования.

Как отмечено выше, коммуникационная парадигма ICN не зависит строго от сквозных потоков, поскольку содержимое можно получить из кэшей в сети. Традиционная концепция потока становится не совсем применимой, поскольку субпотоки или flowlet могут формироваться «на лету», когда части NDO передаются из сетевых кэшей. Для протокола транспортного уровня это сложно, поскольку относящиеся к потоку измерения, традиционно выполняемые транспортным протоколом, таким как TCP, часто могут вводить в заблуждение. Например, некорректные измерения времени кругового обхода (Round-Trip Time или RTT) приведут к значительным различиям средних и сглаженных RTT, что будет вызывать ложные тайм-ауты.

Кроме того, предполагается, что нарушение порядка доставки будет частым в случаях извлечения объекта из сетевых кэшей, а не от исходного источника. В прошлом для TCP было предложено несколько методов работы с нарушением порядка доставки, часть которых можно изменить для применения в контекте ICN. Однако в этом направлении нужны дополнительные исследования для корректного выбора метода и его настройки в соответствии с требованиями архитектуры ICN и применяемого транспортного протокола.

ICN даёт маршрутизаторам возможность объединять запросы и использовать несколько путей, а это значит, что не существует такого понятия как (выделенный) сквозной путь. Например, маршрутизатор, получивший одновременно два запроса для одного содержимого, передаст своему соседу лишь один запрос. Объединение запросов оказывает общее влияние на устройство транспортного протокола и предлагает несколько новых вариантов реализации стратегии пересылки на уровне узла и переосмысления совместного использования ресурсов в сети [RESOURCE-POOL].

Обеспечение беспристрастности для запрашивающих может быть одной из проблем, поскольку невозможно определить число запрашивающих, стоящих за конкретным запросом. Другой проблемой, связанной с объединением запросов, является управление повторной передачей запросов. Обычно предполагается, что маршрутизатор не будет повторять запрос, если он передал недавно идентичный запрос, а по причине отсутствия сведений о запрашивающем маршрутизатор не может отличить исходный запрос клиента от повтора от того же клиента. В таких случаях маршрутизаторы могут приспособить свои таймеры для использования лучшего из коммуникационных путей.

4.7. Кэширование в сети

Явное именование объектов данных позволяет кэшировать их практически в любом элементе сети, включая маршрутизаторы, кэширующие прокси и устройства конечных пользователей. Поэтому кэширование в сети может повысить производительность за счёт извлечения содержимого на узлах, расположенных ближе к конечному пользователю. В части кэширования в сети было отмечено несколько проблем, требующих исследования. Далее рассмотрены важные вопросы, связанные со свойствами новой системы повсеместного кэширования.

4.7.1. Размещение кэша

Снижение стоимости быстрой памяти даёт возможность реализовать кэш в маршрутизаторах и воспользоваться преимуществами кэширования NDO. Мы выделяем два подхода к кэшированию в сети - на пути и вне пути. Оба подхода должны учитывать проблему расположения кэша. Кэширование вне пути похоже на традиционное прокси-кэширование или размещение сервера CDN. Извлечение содержимого из кэша вне пути требует перенаправления запросов и поэтому тесно связано с рассмотренной ниже проблемой маршрутизации по запросам к кэшу. Кэши off-path размещаются в стратегических точках сети, чтобы сократить задержки на перенаправление и число окольных интервалов (hop) для извлечения кэшированного содержимого. Здесь могут помочь исследования, выполненные для кэширующих прокси и CDN.

С другой стороны, кэширование на пути требует меньшего вмешательства в сеть и более подходит для ICN. Однако такое кэширование требует работы со скоростью линии, что вносит больше ограничений в устройство и работу кэширующих элементов сети. Кроме того, выигрыш от таких систем сетевого кэширования на пути зависит от попадания в кэш и по этой причине является ограниченным преимуществом с учётом огромного объёма содержимого в Internet. По этой причине сетевые операторы могут изначально рассматривать лишь ограниченное число элементов сети для реализации на них сетевого кэширования. Выбор узлов для установки кэшей является открытым вопросом и может основываться среди прочего на топологических критериях или характеристиках трафика. Эти вопросы связаны с рассматриваемыми ниже проблемами размещения кэша и маршрутизации по запросам к кэшу.

Однако в большинстве случаев реализацию, развёртывание и работу сетевых кэшей определяет стоимость. Работа кэша со скоростью линии неизбежно требует быстрой памяти, что повышает стоимость реализации. В зависимости от инвестиций ISP может потребоваться принять стратегические решения о размещении кэшей, которое может зависеть от нескольких факторов, таких как исключение дорогих и междоменных каналов, близость узлов к центру, размер домена, пространственное распределение пользователей и картины трафика в конкретной части сети (например, университет, предприятие, модный район города).

4.7.2. Распространение содержимого по кэшам

С учётом числа элементов кэширования (на и вне пути) в сети, на распределение содержимого в кэш будет влиять динамика системы в части перенаправления запросов (в основном для кэширования вне пути) и выигрыш системы в части попадания в кэш. Прямой подход к размещению содержимого - это размещение на пути от источника к получателю. Это снижает расчётные и коммуникационные издержки размещения содержимого в сети. Но может снизить шансы попадания в кэш. Это связано с проблемой маршрутизации по запросам к кэшу, рассмотренной ниже.

Кроме того с числом реплик в системе связаны проблемы управления ресурсами в части размещения кэшей. Например, непрерывная репликация объектов данных во всех элементах сети приводит к избыточному числу копий

объекта. Проблема избыточных реплик была исследована ранее для иерархических web-кэшей. Однако в иерархическом кэшировании web наложенная система координации между плоскостями данных и управления гарантирует рост производительности в части попадания в кэш. Сетевое кэширование на пути со скоростью линии предъявляет иные требования, поэтому нужно исследовать новые методы. К этому относится, в частности снижение уровня избыточности кэшированных копий. Однако вопрос координированного размещения содержимого в кэшах на пути остаётся открытым.

Проблема распределения содержимого в кэш связана также с характеристиками кэшируемого содержимого. Для популярных сведений может потребоваться размещение там, где содержимое будет запрошено в следующий раз. Кроме того, вопросы «ожидаемой популярности содержимого» или временного размещения требуется учитывать при разработке алгоритмов сетевого кэширования, чтобы некоторые сведения получали приоритет (популярное содержимое в сравнении с одноразовым). Критерии установки приоритета для содержимого также связаны с деловыми отношениями между провайдерами и сетевыми операторами. Вопросы бизнес-модели будут влиять на размещение содержимого в кэше, но это выходит за рамки документа.

4.7.3. Маршрутизация по запросам к кэшу
Чтобы воспользоваться кэшированным содержимым, нужно пересылать запросы узлам, имеющим в кэше соответствующие сведения. Эта проблема связана с маршрутизацией по именам, рассмотренной выше. В идеале запросы должны следовать по пути к кэшированному NDO. Однако сведения о расположении содержимого в кэше не могут широковещательно передаваться через сеть. Поэтому сведения о размещении NDO на момент запроса могут отсутствовать или быть неточны (т. е. содержимое может быть уже удалено к моменту перенаправления запроса узлу).

Координация между плоскостями данных и управления для обновления сведений о кэшированном содержимом рассматривалась, но в этом случае возникает проблема расширяемости. Фактически имеется два варианта. Можно полагаться на кэширование с учётом обстоятельств (opportunistic), где запросы пересылаются серверу и при обнаружении NDO на пути, содержимое извлекается из данного узла а не исходного сервера, либо применяется маршрутизация с учётом кэша. Такая маршрутизация может включать обе плоскости данных и управления или одну из них. Кроме того, маршрутизация с учётом кэширования может быть выполнена в масштабе домена или включать более одной автономной системы (Autonomous System или AS). В последнем случае может потребоваться учёт деловых взаимоотношений между AS для построения расширяемой модели.

4.7.4. Обнаружение несвежести кэшированных NDO
По причине большого числа копий NDO в сетевых кэшах от ICN требуется алгоритм проверки старения, обеспечивающий синхронизацию NDO, размещённых у их провайдеров и в точках сетевого кэширования. Для решения этой задачи можно рассматривать прямой и косвенный подход.

При прямом подходе каждый кэш ищет определённую информацию в имени NDO (например временную метку), которая напрямую указывает устаревание. Этот подход применим к некоторым NDO, возникающим при межмашинном взаимодействии и в прилодениях Internet вещей, где базовые операции полагаются на получение последней версии NDO (например, датчики на ферме предоставляют различные параметры, которые передаются на дисплей или в систему регулирования теплицы) [FRESHNESS].

При непрямом подходе каждый кэш обращается к издателю кэшированного NDO для решения вопроса об устаревании до обслуживания. Этот подход предполагает, что NDO включает сведения об издателе, которые позволяют достичь того. Это подходит для NDO, срок действия которых трудно установить заранее, например, для web-страниц, содержащих основной текст (остаётся неизменным) или интерактивных разделов, таких как комментарии или реклама (обновляются нерегулярно).

Часто утверждают, что игнорирования устаревших NDO в кэшах и простого предоставления новых имён для обновлённых NDO может быть достаточно без использования механизмов устаревания. Однако уведомление пользователей об именах обновлённых NDO является нетривиальной задачей. Если обновление не передать одновременно всем пользователям, некоторые продолжат работу со старым именем, хотя им нужен новый NDO.

Одной из задач исследования является разработка моделей согласованности и когерентности для кэшированных NDO вместе с обработкой версий и протоколами обновления, обеспечивающими расширяемость.

4.7.5. Совместное использование кэша несколькими приложениями
Когда ICN развёрнута как независимая от приложений сеть общего назначения и инфраструктура кэширования, множество потребителей и издателей (представляющих разные приложения) будут взаимодействовать в рамках одной инфраструктуры. С универсальными схемами именования и достаточно уникальными идентификаторами на основе хэш-значений, разные приложения могут прозрачным способом совместно использовать идентичные NDO.

В зависимости от подходов к именованию, целостности данных и проверки подлинности источников могут возникать технические или бизнес-проблемы при совместном использовании кэша разными приложениями, такими как защита содержимого, предотвращение отравления кэшей, обеспечение изоляции производительности и т. п. По мере исследования ICN проблемы следует рассматривать и решать в отдельных специализированных документах.

4.8. Управление сетью
Управление сетями было основным делом в основанной на IP, ориентированной на хосты парадигме с тех пор, как эта технология была представлена в «производственных» сетях. Однако на заре IP, управление рассматривалось прежде всего как надстройка. Важнейшие инструменты, повседневно применяемые в сети, такие как ping и traceroute, не были широко доступными более десяти лет с момента внедрения IP. Протоколы управления, такие как SNMP, стали доступны намного позже IP и многие до сих пор считают их недостаточными, несмотря на многолетний опыт применения в ориентированных на хосты сетях. Сегодня, когда развёртывается много новых сетей, сетевое управление считается ключевым аспектом для любого оператора, что создаёт серьёзную проблему, которая при отсутствии должного решения может напрямую повышать расходы сетевого оператора . Если мы хотим развёртывать ICN в инфраструктурных сетях, разработка средств и механизмов управления должна идти рука об руку с разработкой архитектуры.

Хотя определение модели управления FCAPS[1] [ISOIEC-7498-4] для ICN явно выходит за рамки документа, нужно создать базовые инструменты для ICN в целом на ранних этапах разработки и экспериментов, чтобы развивать их в помощь сетевым операционным центрам (network operations center или NOC) для задания правил, проверки их применения на практике, своевременного уведомления об отказах, поиска и решения конфигурационных проблем. Необходимо также рассматривать AAA[2] и управление производительностью с точки зрения NOC. С учётом ожидания большого числа узлов и непредсказуемого объёма трафика предпочтительна автоматизация задач и даже применение механизмов самоуправления. Основная проблема здесь состоит в том, что имеющиеся инструменты ориентированы на хосты и сквозные соединения или предполагают коммуникационную среду с потоками пакетов. Переосмысление достижимости и операционной доступности, например, может дать важные сведения об управлении ориентированными на информацию сетями в будущем.

В части управления сетью мы видим три аспекта. Во-первых, любому оператору нужно управлять всеми доступными в сети ресурсами от подключения узлов до доступности пропускной способности, сетевых хранилищ и множественного доступа. В ICN пользователи будут привносить в сеть значимые ресурсы в плане расширения покрытия, хранилищ и возможностей обработки. Следует рассматривать также характеристики DTN, насколько это возможно (например, распространение содержимого через машины данных - mule). Во-вторых, с учётом того, что узлы и каналы не являются центральными элементами ICN, для управления сетью следует применять естественные механизмы ICN. Например, сетевые хранилища и распознавание имён могут служить для мониторинга, а естественные функции публикации и подписки - для инициирования уведомлений. В-третьих, поддержка является ядром функций управления сетью, позволяя контролировать и выполнять операционные действия и активировать сеетвые процедуры оптимальным путём. Например, аспекты мониторинга могут согласованно сопрягаться, позволяя согласованному исполнению операций.

Однако соображения по применению внутренних механизмов и возможностей ICN для поддержки операций управления выходят за рамки простого сопоставления. Фактически это не только создаёт ряд проблем, но и открывает новые возможности как для ICN, так и для управления сетью как концепции. Например. Механизмы именования занимают центральное место во внутренних операциях ICN, которые служат для идентификации и доступа к содержимому в разных аспектах (например, иерархические и «плоские» имена). Таким способом ICN отделяется от ориентированных на хосты аспектов, на которых основаны традиционные схемы управления. Поэтому возникают вопросы, которые можно напрямую транслировать в задачи управления сетью, такие как способы адресации узлов или сегментов сети в парадигме именования ICN, способы идентификации подключения узлов и выяснения их возможностей (например, узел со слабым или сильным межмашинным взаимодействием M2M) и наличие ориентированного на хосты протокола, работающего там, где может также применяться процесс управления.

С другой стороны, те же присущие ICN характеристики позволяют посмотреть на управления сетью с иной точки зрения. Сосредоточив операции на NDO, можно представить новые операции управления, касающиеся, например, управления или контроля доступа на уровне содержимого, а также анализа производительности на уровне NDO, а не канала или узла. Более того, такие соображения можно применить для управления операционными аспектами самих механизмов ICN. Например, в [NDN-MGMT] реализовано использование ориентированных на содержимое возможностей CCN для управления оптимальной связностью каналов для узлов в сочетании с процессом оптимизации сети. И наоборот, то, как эти ориентированные на содержимое аспекты могут иначе влиять на управление в других областях (например, безопасность и отказоустойчивость) также важно, как показано в [CCN-ACCESS], ге механизмы контроля доступа интегрированы в прототип архитектуры [PURSUIT].

Основные направления исследований в части управления ICN перечислены ниже.

- Управление и контроль за приёмом NDO у запрашивающей стороны.
- Координация обмена данными управления и контроля между узлами ICN и точками управления сетью ICN.
- Идентификация действий и элементов управления и контроля путём именования информации.
- Взаимосвязи между NDO и идентификацией хостов, например, способы идентификации конкретного канала, интерфейса или потока, требующего управления.

4.9. Применение ICN

ICN подходит для различных областей применения и ожидается обеспечение преимуществ для разработчиков приложений за счёт предоставления более подходящих интерфейсов в дополнение к описанным выше преимуществам ICN. В [RFC7476] представлен обзор областей применения в целом. В этом разделе рассмотрены возможности и проблемы для нескольких областей применения.

4.9.1. Web-приложения

Интуитивно понятно, что стиль ICN «запрос-отклик» напрямую отображается на web-коммуникации по протоколу HTTP. Имена NDO могут служить эквивалентом URI в современной системе web, фирменное или прозрачное кэширование можно заменить сетевым кэшированием ICN, а разработчики могут напрямую использовать ICN API для запросов и откликов при создании приложений.

В таких исследованиях, как [ICN2014-WEB-NDN], анализировались реальные web-приложения и способы их реализации в ICN. Наиболее важным результатом стало понимание того, что взаимодействия в стиле REST-style (Representational State Transfer) в значительной степени зависят от передачи контекста пользователя (приложения) в запросах HTTP GET, которые будут отображаться в соответствующие сообщения ICN. Проблемой ICN является способ такого сопоставления. Это можно сделать, расширив формат имён или структуру сообщений для включения файлов cookie или иных сведений о контексте. Проектные решения должны учитывать издержки в маршрутизаторах (например, при сохранении больших запросов GET/Interest в соответствующих таблицах маршрутизаторов).

Другие проблемы включают возврат различных результатов основанных на зависящей от запрашивающего обработке при наличии неизменяемых объектов (и привязок имён к объектам) в ICN и возможности эффективного двухстороннего обмена, для чего нужен механизм именования и доступа в приложению запрашивающего.

[1] Fault, Configuration, Accounting, Performance, and Security - отказы, настройка, учёт, производительность, безопасность.
[2] Authentication, Authorization, and Accounting - проверка подлинности и полномочий, учёт.

4.9.2. Видеопотоки и загрузка

Одним из основных применений ICN является передача и загрузка видеопотоков, где доступ к именованным данным, защита на уровне объекта и сетевые хранилища могут удовлетворять требованиям обеих задач. Применимость и преимущества ICN для видео были продемонстрированы в нескольких прототипах реализаций [ICN2014-AHLGREN-VIDEO-DEMO]. В [VIDEO-STREAMING] рассмотрены возможности и проблемы применения таких видео-служб, как DASH (Dynamic Adaptive Streaming over HTTP) для потоков и загрузки в ICN с учётом требований производительности, взаимосвязи с одноранговыми потоками «вживую», IPTV, и DRM (Digital Rights Management). Помимо простого переноса современных видеоприложений из ориентированной на хосты парадигмы в ICN, имеются многообещающие возможности применения сетевых служб ICN для переустройства и существенного улучшения доступа и распространения видео [ICNRG-2015-01-WESTPHAL]. Например, хранение и пересылка в ICN могут служить для адаптации скорости с целью достижения оптимального QoE (Quality of Experience) в ситуациях с разными свойствами каналов, если данные о пропускной способности возвращаются алгоритмам контроля скорости у отправителя. В сети возможна такая оптимизация, как более активная предварительная выборка за счёт применения видимости блока имён и метаданных NDO в сети. Кроме того, адаптация скорости нескольких источников вместе с сетевым кодированием могут улучшить QoE, например, при доступе через несколько интерфейсов, если есть несколько путей от клиента к восходящим кэшам [RFC7476].

4.9.3. Internet вещей

Сутью ICN является маршрутизация по именам, позволяющая пользователям извлекать NDO независимо от их местоположения. ICN по определению хорошо подходит для приложений IoT, где пользователи потребляют данные, создаваемые из IoT без поддержки защищённых соединений. Базовые API в ICN позволяют разработчикам легко и быстро создавать приложения IoT. Текущие работы, такие как [ICN-FOR-IOT], [ICN-ARCH], [ICN2014-NDNWILD] направлены на выполнение требований ICN для IoT. Например, многие приложения IoT зависят от модели PUSH, где передачу данных инициирует издатель, что делает возможными приложения в реальном масштабе времени (сигналы оповещения и т. п.). Однако ICN не включает естественной поддержки модели PUSH, поскольку та ориентирована на управление передачей данных от получателя. Проблема состоит в эффективной поддержке модели PUSH в ICN, с предоставлением API для публикации и подписки разработчикам приложений IoT. Это можно сделать путём введения других типов идентификаторов, таких как идентификаторы устройств, или расширением взаимодействия запрос-отклик, что может сильно загрузить на маршрутизаторы ICN. Кроме того, ключевые параметры базовых операций ICN также влияют на важные аспекты IoT, такие как кэширование в хранилище содержимого сетевых элементов пересылки. Это позволяет упростить разработку приложений IoT для ICN. Поскольку сеть может работать с именованными объектами, базовые имена обеспечивают способ адресовать содержимое независимо от технологии базовых устройств (и доступа), а расход полосы оптимизируется за счёт возможности кэширования объектов. Однако это создаёт проблемы, связанные со свежестью данных, полученных из кэша, а не от датчика напрямую, поскольку датчики выталкивают содержимое на конкретные узлы (например, для управления ими), что требует индивидуальных адресов для идентификации. Кроме того, разнотипность узлов IoT не позволяет в некоторых случаях обрабатывать содержимое с проверкой подписей.

5. Вопросы безопасности

Документ не влияет на безопасность Internet. Вопросы безопасности, связанные с ICN, рассмотрены в параграфе 4.2.

6. Литература

[ACCESS-CTL-DEL] Fotiou, N., Marias, G., and G. Polyzos, "Access control enforcement delegation for information-centric networking architectures", Proceedings of the second edition of the ICN workshop on Information-centric networking (ICN '12) Helsinki, Finland, DOI 10.1145/2342488.2342507, 2012.

[BACKSCATTER] Waehlisch, M., Schmidt, TC., and M. Vahlenkamp, "Backscatter from the Data Plane - Threats to Stability and Security in Information-Centric Network Infrastructure", Computer Networks Vol 57, No. 16, pp. 3192-3206, DOI 10.1016/j.comnet.2013.07.009, November 2013.

[BREADCRUMBS] Rosensweig, E. and J. Kurose, "Breadcrumbs: Efficient, Best-Effort Content Location in Cache Networks", In Proceedings of the IEEE INFOCOM 2009, DOI 10.1109/INFCOM.2009.5062201, April 2009.

[CCN] Jacobson, V., Smetters, D., Thornton, J., Plass, M., Briggs, N., and R. Braynard, "Networking Named Content", CoNEXT 2009, DOI 10.1145/1658939.1658941, December 2009.

[CCN-ACCESS] Fotiou, N., Marias, G., and G. Polyzos, "Access control enforcement delegation for information-centric networking architectures", In Proceedings of the second edition of the ICN workshop on Information-centric networking (ICN '12), ACM, New York, NY, USA, 85-90, DOI 10.1145/2342488.2342507, 2012.

[CHAUM] Chaum, D. and E. van Heijst, "Group signatures", In Proceedings of EUROCRYPT, DOI 10.1007/3-540-46416-6_22, 1991.

[COMPACT] Cowen, L., "Compact routing with minimum stretch", In Journal of Algorithms, vol. 38, pp. 170-183, DOI 10.1006/jagm.2000.1134, 2001.

[CONTUG] Arianfar, S., Nikander, P., Eggert, L., Ott, J., and W. Wong, "ConTug: A Receiver-Driven Transport Protocol for Content-Centric Networks", Technical Report Aalto University Comnet, 2011.

[DONA] Koponen, T., Ermolinskiy, A., Chawla, M., Kim, K., gon Chun, B., and S. Shenker, "A Data-Oriented (and Beyond) Network Architecture", In Proceedings of SIGCOMM 2007, DOI 10.1145/1282427.1282402, August 2007.

[ENCRYPTION-AC] Kurihara, J., Uzun, E., and C. Wood, "An Encryption-Based Access Control Framework for Content-Centric Networking", IFIP Networking 2015, Toulouse, France, DOI 10.1109/IFIPNetworking.2015.7145300, September 2015.

[FRESHNESS] Quevedo, J., Corujo, D., and R. Aguiar, "Consumer Driven Information Freshness Approach for Content Centric Networking", IEEE INFOCOM Workshop on Name-Oriented Mobility Toronto, Canada, DOI 10.1109/INFCOMW.2014.6849279, May 2014.

[GREEDY] Papadopoulos, F., Krioukov, D., Boguna, M., and A. Vahdat, "Greedy forwarding in dynamic scale-free networks embedded in hyperbolic metric spaces", In Proceedings of the IEEE INFOCOM, San Diego, USA, DOI 10.1109/INFCOM.2010.5462131, 2010.

[HRICP] Carofiglio, G., Gallo, M., and L. Muscariello, "Joint hop-by-hop and receiver-driven interest control protocol for content-centric networks", In Proceedings of ACM SIGCOMM ICN 2012, DOI 10.1145/2342488.2342497, 2012.

[ICN-ARCH] Zhang, Y., Raychadhuri, D., Grieco, L., Baccelli, E., Burke, J., Ravindran, R., Ed., and G. Wang, "ICN based Architecture for IoT - Requirements and Challenges", Work in Progress, draft-zhang-iot-icn-challenges-02, August 2015.

[ICN-FOR-IOT] Lindgren, A., Ben Abdesslem, F., Ahlgren, B., Schelen, O., and A. Malik, "Applicability and Tradeoffs of Information-Centric Networking for Efficient IoT", Work in Progress, draft-lindgren-icnrg-efficientiot-03, July 2015.

[ICN2014-AHLGREN-VIDEO-DEMO] Ahlgren, B., Jonasson, A., and B. Ohlman, "Demo Overview: HTTP Live Streaming over NetInf Transport", ACM SIGCOMM Information-Centric Networking Conference Paris, France, DOI 10.1145/2660129.2660136, September 2014.

[ICN2014-NDNWILD] Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T., and M. Waehlisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild", ACM SIGCOMM Information-Centric Networking Conference Paris, France, DOI 10.1145/2660129.2660144, September 2014.

[ICN2014-WEB-NDN] Moiseenko, I., Stapp, M., and D. Oran, "Communication Patterns for Web Interaction in Named Data Networking", ACM SIGCOMM Information-Centric Networking Conference Paris, France, DOI 10.1145/2660129.2660152, September 2014.

[ICNNAMING] Ghodsi, A., Koponen, T., Rajahalme, J., Sarolahti, P., and S. Shenker, "Naming in Content-Oriented Architectures", In Proceedings ACM SIGCOMM Workshop on Information-Centric Networking (ICN), DOI 10.1145/2018584.2018586, 2011.

[ICNRG-2015-01-WESTPHAL] Westphal, C., "Video over ICN", IRTF ICNRG Meeting Cambridge, Massachusetts, USA, January 2015, <http://www.ietf.org/proceedings/interim/2015/01/13/icnrg/slides/slides-interim-2015-icnrg-1-0.pptx>.

[ICNSURVEY] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and B. Ohlman, "A Survey of Information-Centric Networking", In Communications Magazine, IEEE, vol. 50, no. 7, pp. 26-36, DOI 10.1109/MCOM.2012.6231276, 2012.

[ISOIEC-7498-4] ISO, "Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management Framework", November 1989, <http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip>.

[MANI] Pentikousis, K. and T. Rautio, "A multiaccess Network of Information", WoWMoM 2010 IEEE, DOI 10.1109/WOWMOM.2010.5534922, June 2010.

[MDHT] D'Ambrosio, M., Dannewitz, C., Karl, H., and V. Vercellone, "MDHT: A hierarchical name resolution service for information-centric networks", ACM SIGCOMM workshop on Information-centric networking Toronto, Canada, DOI 10.1145/2018584.2018587, August 2011.

[MMIN] Pentikousis, K. and P. Bertin, "Mobility management in infrastructure networks", Internet Computing, IEEE vol. 17, no. 5, pp. 74-79, DOI 10.1109/MIC.2013.98, October 2013.

[NDN-CTL-SHARING] Yu, Y., "Controlled Sharing of Sensitive Content", IRTF ICNRG Meeting San Francisco, USA, October 2015, <https://www.ietf.org/proceedings/interim/2015/10/03/icnrg/slides/slides-interim-2015-icnrg-4-8.pdf>.

[NDN-MGMT] Corujo, D., Aguiar, R., Vidal, I., and J. Garcia-Reinoso, "A named data networking flexible framework for management communications", Communications Magazine, IEEE vol. 50, no. 12, pp. 36-43, DOI 10.1109/MCOM.2012.6384449, December 2012.

[PURSUIT] Fotiou et al., N., "Developing Information Networking Further: From PSIRP to PURSUIT", In Proceedings of Proc. BROADNETS. ICST, DOI 10.1007/978-3-642-30376-0_1, 2010.

[RANDOM] Gkantsidis, C., Mihail, M., and A. Saberi, "Random walks in peer-to-peer networks: algorithms and evaluation", In Perform. Eval., vol. 63, pp. 241-263, DOI 10.1016/j.peva.2005.01.002, 2006.

[RESOURCE-POOL] Psaras, I., Saino, L., and G. Pavlou, "Revisiting Resource Pooling: The case of In-Network Resource Sharing", ACM HotNets Los Angeles, USA, DOI 10.1145/2670518.2673875, October 2014.

[RFC2002] Perkins, C., Ed., "IP Mobility Support", RFC 2002, DOI 10.17487/RFC2002, October 1996, <http://www.rfc-editor.org/info/rfc2002>.

[RFC4838] Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture", RFC 4838, DOI 10.17487/RFC4838, April 2007, <http://www.rfc-editor.org/info/rfc4838>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", RFC 5944, DOI 10.17487/RFC5944, November 2010, <http://www.rfc-editor.org/info/rfc5944>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <http://www.rfc-editor.org/info/rfc6920>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <http://www.rfc-editor.org/info/rfc7476>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <http://www.rfc-editor.org/info/rfc7696>.

[SEEN] Pentikousis, K., "In search of energy-efficient mobile networking", Communications Magazine, IEEE vol. 48 no. 1, pp. 95-103, DOI 10.1109/MCOM.2010.5394036, January 2010.

[VIDEO-STREAMING] Westphal, C., Ed., Lederer, S., Posch, D., Timmerer, C., Azgin, A., Liu, S., Mueller, C., Detti, A., Corujo, D., Wang, J., Montpetit, M., Murray, N., Azgin, A., and S. Liu, "Adaptive Video Streaming over ICN", Work in Progress[1], draft-irtf-icnrg-videostreaming-08, April 2016.

Благодарности

Авторы признательны Georgios Karagiannis за предложения по исследованию QoS, Dimitri Papadimitriou за отклики к разделу о маршрутизации, Joerg Ott и Stephen Farrell за рецензирование всего документа.

Адреса авторов

Dirk Kutscher (редактор)
NEC
Kurfuersten-Anlage 36
Heidelberg
Germany
Email: kutscher@neclab.eu

Suyong Eum
Osaka University, School of Information Science and Technology
1-5 Yamadaoka, Suita
Osaka 565-0871
Japan
Phone: +81-6-6879-4571
Email: suyong@ist.osaka-u.ac.jp

Kostas Pentikousis
Travelping
Koernerstr. 7-10
Berlin 10785
Germany
Email: k.pentikousis@travelping.com

Ioannis Psaras
University College London, Dept. of E.E. Eng.
Torrington Place
London WC1E 7JE
United Kingdom
Email: i.psaras@ucl.ac.uk

Daniel Corujo
Universidade de Aveiro
Instituto de Telecomunicacoes, Campus Universitario de Santiago
Aveiro P-3810-193
Portugal
Email: dcorujo@av.it.pt

Damien Saucez
INRIA
2004 route des Lucioles - BP 93
Sophia Antipolis 06902 Cedex
France
Email: damien.saucez@inria.fr

Thomas C. Schmidt
HAW Hamburg
Berliner Tor 7
Hamburg 20099
Germany
Email: t.schmidt@haw-hamburg.de

Matthias Waehlisch
FU Berlin
Takustr. 9
Berlin 14195
Germany
Email: waehlisch@ieee.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 7933. *Прим. перев.*