Internet Research Task Force (IRTF)
Request for Comments: 8793
Category: Informational
ISSN: 2070-1721

B. Wissingh
TNO
C. Wood
University of California Irvine
A. Afanasyev
Florida International University
L. Zhang
UCLA
D. Oran
Network Systems Research & Design
C. Tschudin
University of Basel

June 2020

Information-Centric Networking (ICN): Content-Centric Networking (CCNx) and Named Data Networking (NDN) Terminology

Информационно-ориентированные сети - терминология CCNx и NDN

Аннотация

Информационно-ориентированные сети (ICN[1]) - это новая парадигма, где сетевые коммуникации выполняются путем запроса именованного содержимого (content) вместо отправки пакетов по адресам получателей. Примерами архитектуры ICN являются сети именованных данных (NDN[2]) и контентно-ориентированные сети (CCNx[3]). В этом документе представлен обзор терминологии и определений, которые могут использоваться при описании концепций этих двух реализаций ICN. Имеются и другие архитектуры ICN, не являющиеся частью концепций NDN и CCNx, но они выходят за рамки этого документа. Документ является результатом работы исследовательской группы ICNRG[4].

Статус документа

Документ не содержит проекта какой-либо спецификации (Internet Standards Track) и публикуется с информационными целями.

Документ создан в Internet Research Task Force (IRTF). IRTF публиует результаты связанных с Internet исследований и разработок. Эти результаты могут оказаться не пригодными для реализации. Данный документ RFC выражает согласованную точку зрения ICNRG и IRTF. Документы, одобренные для публикации IRSG, не претендуют на статус стандартов Internet (см. раздел 2 в RFC 7841).

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc8793.

Оглавление

1. Введение....2
2. Набросок общей картины ICN....2
3. Термины....3
3.1. Базовые термины....3
3.2. Термины, относящиеся к узлам ICN....3
3.3. Термины, связанные с пересылкой....3
3.4. Термины, связанные с типами пакетов....4
3.5. Термины, связанные с типами имен....5
3.6. Термины, связанные с использованием имен....5
3.7. Термины, связанные с безопасностью....5
4. Семантика и применение....6
4.1. Передача данных....6
4.2. Транспортировка данных....6
4.3. Служба поиска....6
4.4. Доступ к базе данных....6

[1]Information-Centric Networking.
[2]Named Data Networking.
[3]Content-Centric Networking.
[4]Information-Centric Networking Research Group - группа исследований по информационно-ориентированным сетям.

4.5. Вызов удаленных процедур....6
4.6. Публикация и подписка....6
5. Взаимодействие с IANA....6
6. Вопросы безопасности....6
7. Литература....7
7.1. Нормативные документы....7
7.2. Дополнительная литература....7

1. Введение

Архитектура ICN является развитием инфраструктуры Internet от имеющихся хост-ориентированных систем в направлении ориентации на данные, где доступ к информации по именам становится важным элементом (примитивом) сетей. Цель заключается в обеспечении приложениям возможности ссылаться на данные независимо от места их размещения или способов доставки, что обеспечивает естественную групповую доставку, повсеместное кэширование в сети и репликацию объектов данных.

Поскольку разработка этого направления продолжается, появляется много новых терминой. Целью данного документа является сбор ключевых терминов с их определениями, применяемыми в проектах CCNx и NDN. Важными для этих проектов документами являются [RFC8569], [RFC8609] и [NDNTLV]. Другие проекты ICN, такие как [NETINF], [PSIRP], [MOBILITY-FIRST] не рассматриваются здесь, но могут быть предметом других документов.

Для обеспечения контекста некоторых из определяемых здесь терминов сначала обрисована общая картина ICN путем введения базовых концепций и указания основных компонентов в разделе 2. Затем в разделе 3 рассматриваются относящиеся к ICN термины, разделенные по категориям. Следует отметить, что при такой организации некоторые термины могут применяться до их определения.

Хотя этот документ описывает термины, связанные с конфиденциальностью и целостностью, следует отметить, что архитектуры ICN, подобные NDN и CCNx, в общем случае не обеспечивают конфиденциальности данных, перенося этот вопрос на уровень приложений.

Документ представляет согласованную точку зрения ICNRG. Он широко обсуждался членами исследовательской группы (RG[1]), занимающимися конкретными направлениями, рассматриваемыми в документе. Документ не является результатом работы IETF и не предназначен для стандартизации в IETF.

2. Набросок общей картины ICN

В сетевом смысле ICN является инфраструктурой для доставки именованных данных, более полное описание которой дано в разделе 4.

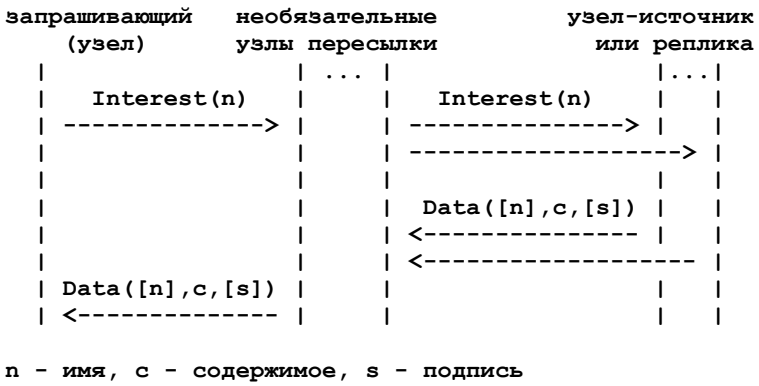

Рисунок 1. Протокол "запрос-отклик в сети ICN.

Ниже описаны базовые концепции, требуемые для обсуждения реализации этой абстракции услуг.

Request-Reply Protocol (пакеты Interest и Packet) - протокол “запрос-отклик”

Услуги поиска в ICN реализуются через определение двух форматов сетевых пакетов - Interest с запросом содержимого по имени и Data с запрошенным содержимым. Возвращаемые пакеты Data должны соответствовать параметрам запроса (например, полное или частичное совпадение имени). Если запрос не однозначен и ему соответствует несколько пакетов Data, сеть ICN возвращает лишь один подходящий пакет Data (это балансирует пакеты Interest и Data через отдельный интерфейс L2).

Packet and Content Names - пакеты и имена содержимого

Без строгой криптографии привязка имени пакета данных к его содержимому будет бесполезна при выборке конкретной информации. В ICN привязка содержимого пакетов Data к имени выполняется криптографически с помощью (1) подписи, явно привязывающей выбранное приложением имя к содержимому пакетов Data или (2) на основе неявного имени (криптографическое хэш-значение пакета Data с выбранным приложением именем или без него), которое потребитель данных получает иным путем.

Data Authenticity and Encryption - шифрование и аутентичность данных

Любой потребитель или элемент сети может (в принципе) проверить аутентичность пакета Data на основании криптографической привязки между именем и содержимым. Отметим, что аутентичность данных не тождественна доверию к ним, хотя они связаны между собой. Пакет считается аутентичным, если он имеет действительную привязку имени к содержимому, но это не предполагает обязательного «доверия» к нему.

Trust - доверие

Аутентичность данных отличается от доверия к ним, хотя эти концепции связаны. Пакет считается аутентичным при наличии действительной привязки имени к содержимому. Пакет считается доверенным (т. е. происходящим от

[1]Research Group.

«уважаемого» или достоверного источника), если привязка действительна в контексте модели доверия. Модель доверия предполагает доверие к тому, что имя, присвоенное определенной порции данных, действительно для их содержимого. Дополнительно этот вопрос рассматривается в разделе 6.

Segmenting and Versioning - сегментация и версии

В сетях ICN размер пакетов ограничен. Поскольку объекты данных прикладного уровня могут быть достаточно велики, их приходится сегментировать в отдельные пакеты Data. Имена таких пакетов могут, например, создаваться путем выбора общего имени объекта прикладного уровня и суффикса, добавляемого к каждому сегменту. Один и тот же метод может применяться для обслуживания разных версий объекта прикладного уровня путем включения номера версии в имя объекта.

Packet and Frame - пакет и кадр

NDN и CCNx используют протокольные блоки данных (PDU[1]), которые обычно больше максимального передаваемого блока базовой сетевой технологии. Здесь PDU называются пакетами и (возможно фрагментированными) частями пакетов, роходящими через интерфейс L2 с ограниченным MTU как кадры. Обработка на уровне L2, ведущая к фрагментированию пакетов ICN, выполняется внутри сети ICN и не видна сервисному интерфейсу.

ICN Node - узел ICN

Узел в сети ICN может играть роль производителя данных (producer), их потребителя (consumer) и/или пересылающего пакеты Interest и Data. При соединении узла пересылки с соседями он в реальном масштабе времени пересылает пакеты Interest и Data. Этот узел может также служить промежуточным хранилищем, удерживающимна некоторое время пакеты Interest и Data перед их отправкой следующему узлу. На узле ICN могут также применяться протоколы маршрутизации для оказания помощи в пересылке пакетов Interest.

Forwarding Plane - плоскость (уровень) пересылки

Канонический способ реализации пересылки пакетов в сети ICN базируется на 3 структурах данных, фиксирующих состояние узла, - FIB[2], PIT[3] и CS[4]. Применяются также стратегии пересылки Interest, принимающие данные от FIB и измерителей для принятия решений о пересылке Interest. Получив пакет Interest, узел проверяет CS и PIT для поиска подходящей записи. Если такой записи не найдено, узел записывает Interest в свою таблицу PIT и пересылает Interest на следующий интервал (интервалы) по пути к запрошенному содержимому на основе информации из своей базы FIB.

3. Термины

3.1. Базовые термины

Information-Centric Networking (ICN) - информационно-ориентированная сеть

Сетевая архитектура, отыскивающая пакеты данных (Data) в ответ на запросы Interest. Двумя реализациями ICN служат ориентированные на соединения сети CCNx (1.x) и сети именованных данных NDN.

Data Packet Immutability - неизменяемость пакетов данных

После создания пакета Data криптографическая подпись связывает его имя с содержимым, обеспечивая обнаружение изменений, внесенных в имя или содержимое, что позволяет отбрасывать измененные пакеты. Если содержимое пакета Data предназначено для изменения, следует использовать версию в имени для обнозначной идентификации каждого неизменного экземпляра содержимого. Это позволяет устранять неоднозначности разных версий содержимого для обеспечения корддинации экземпляров в распределенной системе.

3.2. Термины, относящиеся к узлам ICN

ICN Interface - интерфейс ICN

Обобщение сетевого интерфейса, которое может представлять физический интерфейс (ethernet, Wi-Fi, bluetooth и т. п.), наложенный канал между узлами (туннель IP/UDP и т. п.) или канал IPC[5] с приложением (сокет unix, общая память и т. п.).

Синоним - face.

ICN Consumer - потребитель ICN

Элемент ICN, запрашивающий пакеты Data путем создания и отправки пакетов Interest в направлении локального (через интерфейс внутри узла) или удаленного (через внешний интерфейс узла) узла пересылки ICN.

Синонимы - consumer, information consumer, data consumer, consumer of the content.

ICN Producer - производитель (издатель) ICN

Элемент ICN, создающий пакеты Data и делающий их доступными для извлечения.

Синонимы - producer, publisher, information publisher, data publisher, data producer.

ICN Forwarder - пересылающий узел ICN

Элемент ICN, реализующий пересылку с учетом состояния.

Синоним - ICN router.

ICN Data Node - узел данных ICN

Элемент ICN, временно сохраняющий и потенциально содержащий пакет Interest или Data перед его пересылкой следующему элементу ICN. Отметим, что такие узлы ICN не обладают всеми свойствами узлов данных, используемыми в спецификации DTN[6] [RFC4838].

3.3. Термины, связанные с пересылкой

Stateful Forwarding - пересылка с учетом состояния

Процесс пересылки, записывающий входящие пакеты Interest в таблицу PIT и использующий записанную информацию для пересылки полученных пакетов Data в направлении потребителей. Записанная информация может также служить для измерения производительности плоскости данных, например, для тонкой настройки стратегии пересылки.

Синонимы - ICN Data plane, ICN Forwarding.

[1]Protocol Data Unit.
[2]Forwarding Interest Base - база пересылки Interest.
[3]Pending Interest Table - таблица ожидающих Interest.
[4]Content Store - хранилище содержимого.
[5]Inter-process communication - коммуникации между процессами на узле.
[6]Delay Tolerant Networking - устойчивая к задержкам сеть.

Forwarding Strategy - стратегия пересылки
Модуль пересылки ICN с учетом состояния (ICN data), принимающие решение о том, куда и как переслать входящий пакет Interest. Стратегия пересылки принимает также данные FIB, параметры производительности плоскости данных и/или использует иные механизмы для принятия решений.
Синоним - Interest forwarding strategy.

Upstream - восходящая (пересылка)
Пересылка пакетов в направлении Interest (т. е. пакеты Interest пересылаются в восходящем направлении - потребитель, маршрутизатора, маршрутизатор, ..., издатель.

Downstream - нисходящая (пересылка)
Пересылка пакетов в направлении, обратном перемылке Interest (пакеты Data и Interest Nacks пересылаются в нисходящем направлении): издатель, маршрутизатор, ..., потребители.

Interest Forwarding - пересылка Interest
Процесс пересылки пакетов Interest с использованием Name из этих пакетов. При пересылке с учетом состояния это включает также создание записи в PIT. Решение о пересылке принимает Forwarding Strategy.

Interest Aggregation - агрегирование Interest
Процесс объединения множества пакетов Interest с одним Name и дополнительными ограничениями для тех же Data в одну запись PIT.
Синоним - Interest collapsing.

Data Forwarding - пересылка данных
Процесс пересылки входящих пакетов Data интерфейсам, указанным в соответствующих записях PIT и удаления этих записей.

Satisfying an Interest - выполнение Interest
Процесс возврата содержимого в целом, удовлетворяющий ограничениям, заданным в Interest (прежде всего, совпадение Name).

Interest Match in FIB (longest prefix match) - совпадение Interest в FIB по самому длинному префиксу
Процесс нахождения записи FIB с наибольшим совпадением префикса (по числу компонентов Name), являющимся префиксом указанного Name (см. 3.5. Термины, связанные с типами имен).

Interest Match in PIT (exact match) - точное совпадение Interest в FIB
Процесс нахождения записи PIT с тем же Name, что указано в Interest (включая ограничения Interest при наличии).

Data Match in PIT (all match) - полное совпадение Data в FIB
Процесс нахождения набора записей PIT, которым может соответствовать указанный пакет Data.

Interest Match in CS (any match) - совпадение Interest в CS
Процесс нахождения записи в Content Store маршрутизатора, соответствующей заданному пакету Interest.

Pending Interest Table (PIT) - таблица ожидающих Interest
База данных с записями полученных, но еще не выполненных Interest с указанием интерфейсов, принявших запросы. PIT может также включать интерфейсы, в которые пересланы Interest, ссылки для доступа к сведениям о производительности плоскости данных. Пакеты Interest до одних Data объединяются в одну запись PIT.

Forwarding Information Base (FIB) - база информации о пересылке
База данных с набором префиксов, каждый из которых связан с одним или несколькими интерфейсами, которые могут использоваться для получения пакетов Data с Name по соответствующему префиксу. Список интерфейсов для каждого префикса может ранжироваться и каждый интерфейс может быть связан с дополнительной информацией, облегчающей принятие решений о пересылке.

Content Store (CS) - хранилище содержимого
База данных для кэширования в маршрутизаторе ICN.

In-Network Storage - хранилище в сети
Необязательный процесс хранения пакетов Data внутри сети (opportunistic cache, dedicated on/off path cache, managed in-network storage system) для выполнения будущих запросов Interest к тем же Data. Хранилища могут анонсировать сохраненные пакеты Data в систему маршрутизации.

Opportunistic Caching
Процесс временного хранения пересланных пакетов Data в памяти маршрутизатора (RAM или диск) для их использования в ответах на будущие Interest для тех же Data.
Синоним - on-path in-network caching.

Managed Caching - управляемое кэширование
Процесс поддержки временного, постоянного или планируемого хранилища избранных пакетов Data.
Синоним - off-path in-network storage.

Managed In-Network Storage - управляемое хранилище в сети
Элемент, выступающий как издатель ICN, который реализует управляемое кэширование.
Синонимы - repository, repo.

ICN Routing Plane - плоскость маршрутизации ICN
Протокол или набор протоколов ICN для обмена информацией о доступности пространства имен (Name).

ICN Routing Information Base (RIB) - информационная база маршрутизации ICN
База данных с набором отображений префикс-интерфейс, создаваемых работой одного или множества протоколов маршрутизации. RIB используется для заполнения FIB.

3.4. Термины, связанные с типами пакетов

Interest Packet - пакет Interest
Пакет сетевого уровня, выражающий запрос пакета Data с использованием точного имени или префикса. Пакет Interest может включать набор дополнительных ограничений (например, селекторы Interest). Можно связать Interest с дополнительной информацией для упрощения пересылки, а также включить в Interest время жизни, число интервалов пересылки, рекомендации по пересылке, метки и т. п. В разных решениях ICN использование такой информации может различаться.
Синонимы - Interest, Interest message, information request.

Interest Nack - негативное подтверждение Interest
Пакет, содержащий пакет Interest и необязательную аннотацию, который передается маршрутизатором ICN интерфейсу или интерфейсам, откуда был принят пакет Interest. Interest служит для информирования нисходящих узлов ICN о невозможности переслать включенный пакет Interest. Аннотация может описывать причину этого.
Синонимы - network NACK, Interest return.

Data Packet - пакет Data

Пакет сетевого уровня, содержащий данные, однозначно определяемые именем и защищенные механизмами криптографической подписи.

Синонимы - data, data object, content object, content object packet, data message, named data object, named data.

Link - привязка

Тип пакета Data, тело которого содержит имя (Name) другого пакета Data. Это внутреннее имя часто является полным, т. е. указывает Packet ID соответствующего пакета Data, но это не является требованием.

Синоним - pointer.

Manifest - манифест

Тип пакета Data, содержащего привязки полного имени для одного или нескольких пакетов Data. Манифесты группируют коллекции связанных пакетов Data с одним Name. Манифесты позволяют разбивать большие объекты Data на отдельные Content Object с одним именем, а также представлять наборы связанных Content Object как форму «каталога» (directory). Дополнительным преимуществом манифестов является снижение издержек на верификацию подписей для каждого пакета Data, упомянутого во внутренних Link. Манифесты обычно содержат дополнительные метаданные, например, размер (в байтах) каждого привязанного пакета Data и криптографический хэш-дайджест всех Data, содержащихся в связанных пакетах Data.

3.5. Термины, связанные с типами имен

Name

Идентификатор пакета Data. Имена в ICN организованы иерархически (последовательность меток) и обычно семантически значимы, что делает их выразительными, гибкими и специфичными для приложения (подобно HTTP URL). Name может кодировать информацию о контексте приложения, семантике, местоположении (топология, география и т. п.), имени сервиса и т. п.

Синонимы - data name, interest name, content name.

Name component - компонент Name

Последовательность байтов, возможно с цифровым указателем типа, представляющая одну метку в иерархически структурированном имени.

Синоним - name segment (as in CCNx).

Packet ID

Уникальный криптографический идентификатор пакета Data. Обычно это криптографический дайджест пакета Data (например, SHA256 [RFC6234]), учитывающая имя, данные, метаинформацию и подпись.

Синоним - implicit digest.

Selector - селектор

Механизм (условие) выбора отдельного пакета Data из коллекции, соответствующего данному пакету Interest, запрашивающему данные с использованием префикса или точного имени.

Синонимы - interest selector, restrictor, interest restrictor.

Nonce

Поле пакета Interest, временно указывающее экземпляр Interest (для данного имени). Отметим, что определение nonce в спецификации NDN не обязательно соответствует всем свойствам nonce из [RFC4949].

Exact Name - точное имя

Имя, указанное в пакете Data, которое обычно однозначно указывает данный пакет Data.

Full Name - полное имя

Точное имя с Packet ID соответствующего пакета Data.

Prefix Name - префикс имени

Name с частью последовательности меток (начиная с первой) из Name в пакете Data.

Синоним - prefix.

3.6. Термины, связанные с использованием имен

Naming conventions - соглашения об именовании

Соглашение, договор или спецификация именования пакетов Data, структурирующие пространство имен.

Синонимы - Naming scheme, ICN naming scheme, namespace convention.

Hierarchically structured naming - иерархически структурированное именование

Схема именования, выделяющая и интерпретирующая Name как последовательность меток (компоненты Name) с иерархической структурой без единого административного корня (узла). Структура обеспечивает полезный контекст для Name.

Синонимы - hierarchical naming, structured naming.

Flat naming - плоское именование

Схема именования, выделяющая и интерпретирующая Name как одну метку (компонент Name) без внутренней структуры. Это можно считать специальным (вырожденным) случаем структурированного именования.

Segmentation - сегментация

Процесс расщепления большого объема информации приложения в набор пакетов Data с уникальными именами. При использовании иерархически структурированных имен каждый пакет Data имеет общий префикс и дополнительный компонент, представляющий номер сегмента (блока).

Синоним - chunking.

Versioning - поддержка версий

Процесс назначения уникального имени (Name) выпуску содержимого в определенном пакете Data. При импользовании в Name с иерархической структурой версия пакета Data может передаваться в отдельной метке Name (например, префикс указывает данные, а уникальный номер - их версию).

Fragmentation - фрагментация

Процесс расщепления PDU на кадры (Frame), которые можно передать через интерфейс L2 с меьшим MTU.

3.7. Термины, связанные с безопасностью

Data-Centric Security - защита данных

Свойство защиты, связанное с пакетом Data, включая целостность данных, их достоверность (authenticity) и, возможно, конфиденциальность. Эти свойства защиты остаются с пакетом Data независимо от места хранения и способа извлечения.

Синоним - directly securing Data packet.

Data Integrity - целостность данных

Криптографический механизм обеспечения согласованности битов пакета Data. Свойство целостности Data проверяет отсутствие повреждений пакета Data при передаче (например, по ненадежному пути) или в результате намеренного искажения.

Data Authenticity - достоверность данных

Криптографический механизм обеспечения достоверности пакета Data на основе выбранной (например, издателем и/или потребителем) модели доверия. Обычно аутентичность данных обеспечивается за счет использования криптографических подписей с асимметричным шифрованием (например, RSA, ECDSA), но может применяться и симметричное шифрование (например, HMAC[1]) внутри домена доверия.

Data Confidentiality - конфиденциальность данных

Криптографический механизм обеспечения секретности пакета Data. Защита конфиденциальности Data включает раздельные механизмы для содержимого и имени.

Content Confidentiality - конфиденциальность содержимого

Криптографический механизм для предотвращения доступа неуполномоченных сторон к данным в пакете Data. Механизм может быть реализован на основе шифрования (симметричное, асимметричное, гибридное) и соответствующего распространения ключей между уполномоченными сторонами.

Name Confidentiality - конфиденциальность имени

Криптографический механизм, предотвращающий получение мата-информации из пакета Data наблюдателю обмена Interest-Data (например, промежуточному маршрутизатору). Этот механизм может быть реализован на основе шифрования Data (как конфиденциальность содержимого) или «затемнения» (obfuscation).

4. Семантика и применение

Описанная выше терминология является обнародованием предплагаемой семантики операций NDN и CCNx (Wчто ожидается в сети). Далее кратко рассмотрены наиболее часто предлагаемые варианты применения и интерпретации.

4.1. Передача данных

Представление сети NDN и CCNx основано на допущение о том, что протокол запрос-отклик реализует базовые услуги передачи данных без гарантии доставки для одиночных именованных пакетов.

4.2. Транспортировка данных

Передача данных может быть превращена в службу доставки данных для объектов прикладного уровня с помощью дополнительной логики. Эта логика доставки должна понимать и создавать последовательности имен, требуемые для сборки сегментированных объектов. Могут предусматривать разные варианты транспорта (гарантированная доставка, поток, почтовый ящик и т. п.).

4.3. Служба поиска

В более распределенных системном представлении базового протокола запрос-отклик NDN и CCNx обеспечивают распределенную службу поиска, возвращающую значение, найденное по ключу (=name).

4.4. Доступ к базе данных

Услуги поиска можно превратить в протокол доступа к базе данных, используя структуру пространства имен для задания имен в качестве ключей доступа в базу. Следовательно, префикс имени означает коллекцию или таблицу базы данных, а остальная часть имени задает выражение для выполняемого запроса.

4.5. Вызов удаленных процедур

Имена, определенные в этом документе для Interest и Data, могут указывать на вызовы удаленных процедур, их входные аргументы и результаты. Для полного представления о создании RPC и работе с другими системами удаленных вызовов следует обратиться к работе [RICE]. Эти возможности могут быть расширены в полную инфраструктуру распределенной обработки, как предложено в работе [CFN].

4.6. Публикация и подписка

Имена, определенные в этом документе для Interest и Data, могут указывать коллекции даннх, на которые можно подписаться, а также отдельные объекты данных, публикуемые в архитектуре Publish-Subscribe. Пример создания таких систем на основе ICN приведен в работе [LESSONS-LEARNED].

5. Взаимодействие с IANA

Этот документ не предполагает действий IANA.

6. Вопросы безопасности

Хотя определенные здесь термины сами по себе не создают новых вопросов безопасности, использующие эти термины архитекуты могут вызывать такие вопросы. Следует обратиться к спецификации архитектуры (например, [RFC8569] и [NDN]), где вопросы безопасности рассматриваются подробно.

Некоторые из терминов в этом документе используют понятия «доверие» (trust), «заслуживающий доверия» (trustworthy) и «модель доверия» (trust model). Предполагается, что эти термины имеют общепринятый смысл, однако в недавнее время было опубликовано множество работ, посвященных доверию и, в частности, схемам доверия в архитектуре ICN. Например, полезно прочесть работу [SCHEMATIZING-TRUST], где более подробно рассмотрена формализация доверия для современных систем NDN и CCNx.

[1]Hashed Message Authentication Code - хэшированный код аутентификации сообщения.

7. Литература

7.1. Нормативные документы

[CFN] Krol, M., Mastorakis, S., Kutscher, D., and D. Oran, "Compute First Networking: Distributed Computing meets ICN"[1], ACM ICN, DOI 10.1145/3357150.3357395, September 2019, <https://dl.acm.org/citation.cfm?id=3357395>.

[LESSONS-LEARNED] Nichols, K., "Lessons Learned Building a Secure Network Measurement Framework using Basic NDN"[2], ACM ICN, DOI 10.1145/3357150.3357397, September 2019, <https://dl.acm.org/citation.cfm?id=3357397>.

[MOBILITY-FIRST] Raychaudhuri, D., Nagaraja, K., and A. Venkataramani, "MobilityFirst: a robust and trustworthy mobility-centric architecture for the future internet"[3], ACM SIGMOBILE, Volume 16, Issue 3, DOI 10.1145/2412096.2412098, July 2012, <https://dl.acm.org/citation.cfm?id=2412098>.

[NDNTLV] Named Data Networking, "NDN Packet Format Specification", <https://named-data.net/doc/ndn-tlv/>.

[NETINF] Dannewitz, C., Kutscher, D., Ohlman, B., Farrell, S., Ahlgren, B., and K. Holger, "Network of Information (NetInf) - An information-centric networking architecture", Computer Communications, Volume 36, Issue 7, DOI 10.1016/j.comcom.2013.01.009, April 2013, <https://dl.acm.org/citation.cfm?id=2459643>.

[PSIRP] Trossen, D., Tuononen, J., Xylomenos, G., Sarela, M., Zahemszky, A., Nikander, P., and T. Rinta-aho, "From Design for Tussle to Tussle Networking: PSIRP Vision and Use Cases", May 2008, <http://www.psirp.org/files/Deliverables/PSIRP-TR08-0001_Vision.pdf>.

[RICE] Krol, M., Habak, K., Kutscher, D., Oran, D., and I. Psaras, "RICE: remote method invocation in ICN"[4], ACM ICN, DOI 10.1145/3267955.3267956, September 2018, <https://dx.doi.org/10.1145/3267955.3267956>.

[SCHEMATIZING-TRUST] Yu, Y., Afanasyev, A., Clark, D., Claffy, K. C., Jacobson, V., and L. Zhang, "Schematizing Trust in Named Data Networking"[5], ACM ICN, DOI 0.1145/2810156.2810170, September 2015, <https://dx.doi.org/10.1145/2810156.2810170>.

7.2. Дополнительная литература

[NDN] Named Data Networking, "Named Data Networking: Executive Summary", September 2010, <https://named-data.net/project/execsummary/>.

[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, <https://www.rfc-editor.org/info/rfc4838>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC8569] Mosko, M., Solis, I., and C. Wood, "Content-Centric Networking (CCNx) Semantics", RFC 8569, DOI 10.17487/RFC8569, July 2019, <https://www.rfc-editor.org/info/rfc8569>.

[RFC8609] Mosko, M., Solis, I., and C. Wood, "Content-Centric Networking (CCNx) Messages in TLV Format", RFC 8609, DOI 10.17487/RFC8609, July 2019, <https://www.rfc-editor.org/info/rfc8609>.

Благодарности

Marc Mosko предоставил много рекомендаций и точных указаний для правильных формулировок и определений терминов. Marie-Jose Montpetit подготовила рецензию IRSG, что помогло существенно улучшить текст. Дополнительные замечания при опросе IRSG от Stephen Farrell, Ari Keraenen, Spencer Dawkins, Carsten Bormann, Brian Trammell помогли улучшить документ. Полезные комментарии были получены в рамках обзора конфликтов IESG от Mirja Kuehlewind и Benjamin Kaduk.

Адреса авторов

Bastiaan Wissingh

TNO

Email: bastiaan.wissingh@tno.nl

Christopher A. Wood

University of California Irvine

Email: caw@heapingbits.net

[1]Презентация доклада доступна по ссылке. *Прим. перев.*
[2]Полный текст работы доступен по ссылке. *Прим. перев.*
[3]Полный текст работы доступен по ссылке. *Прим. перев.*
[4]Презентация доклада доступна по ссылке. *Прим. перев.*
[5]Полный текст работы доступен по ссылке. *Прим. перев.*

Alex Afanasyev

Florida International University

Email: aa@cs.fiu.edu

Lixia Zhang

UCLA

Email: lixia@cs.ucla.edu

David Oran

Network Systems Research & Design

Email: daveoran@orandom.net

Christian Tschudin

University of Basel

Email: christian.tschudin@unibas.ch

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru