Федеральное государственное автономное
образовательное учреждение высшего образования
«Московский физико-технический институт
(государственный университет)»

На правах рукописи

Трушина Оксана Вячеславовна

Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях

Специальность: 05.13.17 – Теоретические основы информатики

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата физико-математических наук

Научный руководитель
д. т. н., профессор
Габидулин Эрнст Мухамедович

Москва – 2017

Оглавление

Введение

Актуальность темы исследования. Современные системы связи предъявляют высокие требования к обеспечению защиты информации. Дисциплина «защита информации» решает множество вопросов, главным из которых является обеспечение секретности передаваемого сообщения. В конфиденциальности может нуждаться не только передаваемая информация, но также персональная информация отправителя и (или) получателя сообщения и информация о том, между кем происходит передача сообщений. Развитие информационных технологий привело к возникновению нового типа угроз, связанных с несанкционированным доступом к персональным данным. Например, злоумышленник может определить идентификаторы корреспондентов, желающих скрыть факт своего сотрудничества. В связи с этим, обеспечение анонимности в сети представляет собой актуальное и быстро развивающееся направление защиты информации.

Проблему обеспечения анонимности можно разделить на две задачи. Первая задача состоит в том, чтобы секретным образом сформировать маршрут передачи сообщения. Маршрутная информация не должна быть известна злоумышленнику, иначе она даёт ему возможность вычислить идентификаторы корреспондентов. Вторая задача заключается в том, чтобы по установленному маршруту передавать сообщение так, чтобы его нельзя было прослеживать. Это достигается за счёт того, что сообщение, поступившее в некоторый промежуточный узел маршрута, изменяется таким образом, что сообщения на входе и выходе отличаются. Эту задачу называют задачей обеспечения несвязываемости сообщений. Задача обеспечения несвязываемости решается обычно с помощью шифрования. Шифрование осуществляет псевдослучайную перестановку, меняет вид сообщения, сохранив при этом информацию.

Современная криптография основана на предположении, что злоумышленник вычислительно ограничен. Для модели канала с подслушиванием [1, 2] возникло другое направление обеспечения секретности данных. Вместо вычислительных ограничений на злоумышленника накладываются физические ограничения. Предполагается, что злоумышленник не может перехватить сообщение целиком, а только его часть. Другое ограничение состоит в том, что канал, по которому злоумышленник получает сообщение зашумлён больше, чем основной канал передачи. В этих условиях секретности можно достичь без криптографических примитивов, а путём ис-

пользования теоретико-информационных средств, таких как коды.

Такое направление исследований называется теоретико-информационным. В настоящее время ведутся исследовательские работы по обеспечению секретности с использованием модели канала с подслушиванием [3–11]. Для беспроводных сетей задача обеспечения секретности часто ставится на физическом уровне, где методы на основе модели канала с подслушиванием являются основным средством. По сравнению с традиционной криптографией выделяют два важных преимущества теоретико-информационного направления: не существует строгих ограничений на вычислительные ресурсы злоумышленника и нет необходимости решать задачу распределения криптографических ключей, которая может быть довольно сложной и энергозатратной. Первое из этих преимуществ обеспечивает долгосрочную секретность. Второе преимущество существенно для систем связи с маломощными устройствами. Маломощными часто являются портативные устройства, такие как смартфоны.

Подход к обеспечению несвязываемости сообщений определяет в целом подход к обеспечению анонимности передачи данных. Так при теоретико-информационном подходе к несвязываемости можно говорить о теоретико-информационных методах анонимности.

Криптографический подход обеспечивает полный набор методов защиты информации, начиная с секретности сообщений и заканчивая несвязываемостью сообщений. Для того чтобы теоретико-информационный подход смог заменить традиционную криптографию, он также должен предлагать полный набор методов защиты информации. Методы обеспечения секретности на основе модели канала с подслушиванием представлены в литературе, но на данный момент нет методов обеспечения несвязываемости сообщений для такой модели.

В 2000 году был предложен новый способ передачи данных – сетевое кодирование. Этот способ передачи отличается от традиционной маршрутизации тем, что промежуточные узлы могут выполнять определённые алгебраические операции над поступившими пакетами, которые являются элементами конечного поля. Например, составлять их линейные комбинации. Появление сетевого кодирования способствовало развитию исследований не только в области построения новых кодов, но также в области защиты информации, в частности, обеспечения анонимности. Стало понятно, что методы, успешно работающие в традиционных сетях передачи данных и в большинстве своём использующие классическую криптографию, не могут быть применимы к сетевому кодированию, так как не предусматривают выполнение операций с пакетами на внутренних узлах сети. Теоретико-информационные методы защиты информации, основанные на кодах, могут быть встроены в сетевое кодирование более простым способом по сравнению с криптографическими методами, адаптированными для использования в сетевом кодировании.

Таким образом, построение новых эффективных теоретико-информационных методов обеспечения анонимности в сети связи представляет собой актуальную научную задачу как для традиционной маршрутизации данных, так и для сетевого кодирования.

Целью диссертационной работы является построение теоретико-информационных методов несвязываемости на основе модели канала с подслушиванием и исследование их свойств.

Для достижения поставленной цели в работе рассмотрены следующие **задачи**.

1. Разработка и исследование метода обеспечения несвязываемости для цифрового когерентного и аналогового сетевого кодирования.

2. Разработка и исследование метода обеспечения несвязываемости для традиционной маршрутизации.

Научная новизна результатов, полученных в диссертации, заключается в следующем.

1. Построена теоретико-информационная модель обеспечения анонимности, где анонимность определяется с помощью несвязываемости. Предложено понятие совершенной несвязываемости.

2. Впервые разработан и исследован теоретико-информационный метод обеспечения несвязываемости сообщений для цифрового когерентного сетевого кодирования.

3. Впервые разработан и исследован теоретико-информационный метод обеспечения несвязываемости сообщений для традиционной маршрутизации.

4. Впервые разработан и исследован теоретико-информационный метод обеспечения несвязываемости сообщений для аналогового сетевого кодирования.

Теоретическая и практическая значимость. Исследовано применение модели канала с подслушиванием для обеспечения несвязываемости сообщений. Построенные на основе этой модели методы закрывают собой пробел в классе теоретико-информационных методов защиты информации, состоящий в отсутствии теоретико-информационных методов обеспечения анонимности. Показана возможность применения предложенных методов как в беспроводных, так и в проводных сетях.

Положения, выносимые на защиту.

1. Построена теоретико-информационная модель анонимности, где анонимность определяется через несвязываемость. Предложено понятие совершенной несвязываемости.

2. Предложен и теоретически обоснован метод обеспечения несвязываемости сообщений для цифрового когерентного сетевого кодирования, основанный на применении модели канала с подслушиванием.

3. Предложен и теоретически обоснован метод обеспечения несвязываемости сообщений для традиционной маршрутизации, основанный на применении модели канала с подслушиванием.

4. Предложен и теоретически обоснован метод обеспечения несвязываемости сообщений для аналогового сетевого кодирования, основанный на применении модели гауссовского канала с подслушиванием.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих конференциях:

1. Seventh International Workshop on Optimal Codes and Related Topics (Albena, 2013),

2. 56-й научной конференции МФТИ (Долгопрудный, 2013),

3. XIV International Workshop on Algebraic and Combinatorial Coding Theory (Svetlogorsk, 2014),

4. 57-й научной конференции МФТИ (Долгопрудный, 2014),

5. International Conference Engineering & Telecommunications (Dolgoprudny, 2015),

6. XV International Workshop on Algebraic and Combinatorial Coding Theory (Albena, 2016),

7. International Symposium on Problems of Redundancy in Information and Control Systems (St. Petersburg, 2016).

Кроме того, основные результаты докладывались на семинарах кафедры радиотехники и систем управления МФТИ, на семинаре по теории кодирования ИППИ РАН, а также в форме стендового доклада в IEEE European School of Information Theory 2015.

Диссертационная работа является частью работ по гранту РФФИ проекты № 12-07-00122-а и № 15-07-08480-а.

Публикации. По теме диссертации опубликовано 9 работ [13–21], из них 2 в научных журналах, 7 публикаций в трудах научных конференций.

Личный вклад в работах с соавторами. В совместных публикациях научному руководителю Э.М. Габидулину принадлежат постановки задач, а основные результаты и выкладки выполнены диссертантом. В работе [13] соавторам принадлежит аналитический обзор методов секретности, аналитический обзор методов анонимности выполнен диссертантом.

Объем и структура работы. Диссертация состоит из введения, 4 глав и заключения. Общий объем диссертации составляет 102 страницы, включая 19 рисунков, 1 таблицу и список литературы.

Глава 1

Анонимная передача данных

1.1 Введение

Исследования в области анонимной передачи были начаты работой “Untraceable electronic mail return addresses and digital pseudonyms” [22], опубликованной в 1981 году. Система терминов, описывающих анонимную передачу данных, начала формироваться в 2000 году А. Пфицманом. Далее А. Пфицман вместе с соавторами дополнял и усовершенствовал эту систему терминов, которая теперь принята множеством исследователей, занимающихся вопросом анонимной передачи. Последняя версия терминологии была предложена А. Пфицманом в соавторстве с М. Хансеном в 2010 году [23].

Для того чтобы определить анонимность некоторого объекта необходимо предположить наличие множества объектов со схожими характеристиками, которое называют множеством анонимности, а также необходимо определить модель злоумышленника.

Определение 1.1. *Объект называется анонимным с точки зрения злоумышленника, если злоумышленник не может достоверно выделить его среди множества других схожих объектов.*

Определение 1.2. *Пусть до наблюдения за некоторыми объектами у злоумышленника есть предположение о их взаимодействии. Объекты называются несвязываемыми (unlinkable), если после наблюдения за ними предположение злоумышленника не становится более достоверным.*

Для того, чтобы определить, что значит «достоверно» в пункте 1.5 будут рассмотрены численные характеристики анонимности.

Переходя от абстрактного понятия «объект» к практически применимым понятиям отправитель, получатель и сообщение, определим сеть передачи как множество узлов-отправителей,

множество узлов-получателей и множество промежуточных узлов, с помощью которых отправители и получатели могут обмениваться сообщениями. Задача анонимной передачи имеет смысл в сетях, где есть много отправителей, много получателей и в каждый момент времени передается много сообщений. Удобно определять анонимность через несвязываемость. Так можно определить анонимность отправителя как

Определение 1.3. *Отправитель является анонимным, если по отношению к нему каждое передаваемое сообщение является несвязываемым.*

Аналогично можно определить анонимность получателя. Также можно определить *анонимность сеанса связи* (relationship anonymity).

Определение 1.4. *Сеанс связи, то есть процесс передачи сообщения, называется анонимным, если по отношению к этой паре отправитель–получатель каждое передаваемое сообщение является несвязываемым.*

В работе [23] утверждается, что анонимность сеанса связи гарантирует более слабую защиту по сравнению с анонимностью отправителя/получателя. Анонимность отправителя/получателя влечет за собой анонимность сеанса связи. Компрометация анонимности сеанса связи автоматически приводит к компрометации анонимности отправителя/получателя. В тоже время компрометация анонимности отправителя/получателя не приводит к компрометации анонимности сеанса связи. Действительно, если злоумышленник может определить отправителя или получателя сообщения, то анонимность сеанса связи сохраняется пока злоумышленник не может определить второго корреспондента. С другой стороны, сравнивать эти два вида анонимности некорректно, так как они преследуют разные цели. Анонимность сеанса связи не ставит своей задачей защитить отправителя или получателя, но скрыть связь между отправителем и получателем, то есть кто кому передает сообщения.

Задачу анонимной передачи данных можно разделить на две задачи. Первая из них решает задачу секретной маршрутизации. Передаваемые по сети пакеты информации имеют стандартный вид и состоят из преамбулы, содержащей служебную и маршрутную информацию, и данных. В преамбуле в явном виде содержатся идентификаторы отправителя и получателя сообщения, что обеспечивает возможность динамической маршрутизации, но в тоже время компрометирует анонимность. Традиционно эта проблема решается следующим образом. Маршруты устанавливаются статически некоторым секретным способом. То есть таким, при котором маршрутная информация не передается явно по сети. Затем сообщения по этому маршруту передаются одношагово. В этом случае для каждого узла маршрута получателем является следующий за ним узел, а отправителем – он сам. Тогда в преамбуле пакета содержатся идентификаторы смежных узлов, которые в общем случае не являются отправителем и получателем

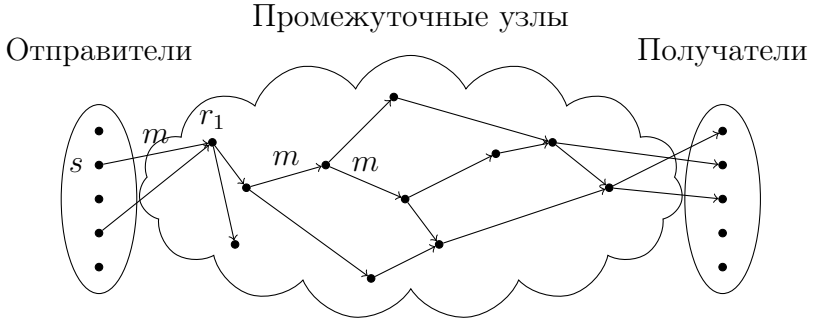


Рис. 1.1: Схема сети передачи данных

сообщения. В таком случае, преамбула не может быть легко использована злоумышленником для компрометации корреспондентов. Но секретной маршрутизации недостаточно для анонимной передачи, так как поле данных не меняется в течение всей передачи по маршруту, тогда на его основе можно прослеживать сообщение. Рассмотрим сеть, представленную на рис. 1.1. Предположим злоумышленник прослушал сообщение m некоторого отправителя. Физически это значит, что злоумышленник прослушал соединение сети между отправителем и следующим узлом маршрута сообщения (соединение $s \to r_1$ на рис. 1.1). Таким образом, злоумышленнику известен следующий передающий узел. Затем он прослушивает все выходные соединения этого узла и сравнивает поле данных пакетов, передающихся по этим соединениям, с полем данных пакета m, подслушанного на предыдущем шаге. Совпадение полей данных однозначно определяет соединение, по которому далее было отправлено сообщение m, а соединение, в свою очередь однозначно определяют следующий узел маршрута. Действуя по этой схеме, злоумышленник может проследить передачу сообщения вплоть до получателя, установив таким образом, кому именно передавал сообщение конкретный отправитель. Эта атака принадлежит широкому классу атак, носящему название *анализ трафика* (traffic analysis). Вторая задача анонимной передачи состоит в противодействии этой атаке. Сообщение по уже установленному маршруту должно передаваться так, чтобы его нельзя было прослеживать на основе его содержимого. Решение состоит в обеспечении *битовой несвязываемости* (bitwise unlinkability). Битовая несвязываемость сообщений гарантирует, что они выглядят по-разному, то есть нельзя найти закономерностей в битовых последовательностях этих сообщений.

Диссертационная работа посвящена обеспечению анонимности сеанса связи, более конкретно, разработке метода обеспечения несвязываемости сообщений. В распределенных сетях анонимность сеанса связи возможно самый востребованный уровень защиты. Пользователи часто не имеют нужды скрывать, что они передают некоторые сообщения, но хотят скрыть информацию о том какие, например, веб-сайты они посещают.

1.2 Модели злоумышленника и возможные атаки

В литературе, посвященной защите информации, устоялись четыре признака, которыми можно охарактеризовать злоумышленника. Модель любого злоумышленника может быть описана набором этих признаков. Перечислим эти признаки.

1. Активность (Capability). Злоумышленник может быть *пассивным* или *активным*. Пассивный злоумышленник может прослушивать сообщения, передаваемые по соединениям сети, а также метаданные, такие как длина сообщения, время поступления сообщения в некоторый узел сети, время выхода сообщения из узла и проводить статистические атаки на основе этих данных. Активный злоумышленник обладает всеми возможностями пассивного злоумышленника, а также способен модифицировать передаваемые сообщения, изымать сообщения из сети или вставлять свои собственные сообщения.

2. Осведомленность (Visibility). Осведомленность злоумышленника определяет к какому количеству соединений сети имеет доступ злоумышленник: сколько соединений сети он может прослушать, на скольких соединениях он может изъять сообщения или вставить свои собственные. Различают *глобального* и *локального* злоумышленников. Глобальный злоумышленник имеет доступ ко всем соединениям сети в то время как локальный – только к некоторому подмножеству соединений. Глобальный злоумышленник может быть смоделирован как некоторое количество взаимодействующих друг с другом локальных злоумышленников.

3. Гибкость (Mobility). Злоумышленников различают по их способности подстраивать проведение атаки к полученной информации. *Адаптивный* злоумышленник на основе уже полученной им информации может определять какие соединения сети ему следует далее использовать для успешного проведения атаки. Например, прослушав выходные соединения некоторого узла и соответственно сообщения, передаваемые по ним, злоумышленник может определить какому именно узлу далее было отправлено интересующее его сообщение. На основе этой информации злоумышленник решает прослушать выходные соединения этого узла, чтобы проследить еще один шаг передачи нужного сообщения. *Статический* злоумышленник до проведения атаки выбирает какие соединения сети он будет использовать и не меняет своей стратегии во время атаки.

4. Вовлеченность (Participation). Злоумышленник может быть *внешним* или *внутренним*. Внутренний злоумышленник участвует в передаче сообщений в роли легального узла сети или компрометирует один или несколько узлов сети так, что имеет доступ ко всем сообщениям, проходящим через эти узлы, а также к способу их обработки внутри узлов. Внешний

злоумышленник напротив никак не участвует в передаче сообщений, но имеет доступ к соединениям сети.

Для систем, обеспечивающих анонимность сеанса связи, наибольшую опасность представляют атаки из класса анализа трафика. Анализ трафика определяют как процесс перехвата и исследования сообщений с целью извлечения полезной информации из профиля сеанса связи. Анализ трафика – это в большинстве своем статистические атаки на основе метаданных. Эти атаки способствуют прослеживанию сообщения вдоль маршрута, что приводит к полной компрометации анонимности сеанса связи.

Первая из этих атак – это атака на основе закономерностей в битовых последовательностях сообщений. Эта атака была рассмотрена ранее на примере, изображенном на рисунке 1.1.

Для проведения атаки злоумышленником могут быть использованы временные характеристики. Регистрируя время поступления сообщений в узел и время выхода сообщений из узла, злоумышленник может связать входящие и выходящие сообщения, зная задержку этого узла, то есть время, которое этот узел тратит на обработку сообщения перед его отправкой. Также для атаки злоумышленник может использовать тот факт, что сообщение, отправляемое источником, разбивается на пакеты, и в сеть передаются пакеты. Злоумышленник может посчитать количество пакетов, отправленных источником некоторому узлу, а также количество пакетов, отправленных этим узлом по каждому из его выходных соединений. То соединение, по которому передаётся такое же количество пакетов, как было отправлено источником, вероятно передает пакеты именно источника. Это позволяет злоумышленнику определить следующий узел маршрута. Анализ пропускной способности соединений также может помочь злоумышленнику найти связь отправителя и получателя [24].

Противодействие атакам на основе метаданных обычно достигается технологическими методами. Например, можно сначала отправлять поступившие сообщения в узлах в буфер, а затем отправлять их не в том порядке, в каком они поступили. Это помогает для предотвратить атаки по временным характеристикам. Только битовая несвязываемость достигается математическими методами. Самый распространённый способ изменить битовую последовательность сообщения и при этом сохранить передаваемую информацию – это шифрование.

1.3 Существующие методы обеспечения анонимности

Существует несколько основных идей, на которых строится множество методов обеспечения анонимности [25, 26]:

1. Mix-net [22].

2. DC-net (Dining Cryptographer Networks) [27].

3. Маршрутизация.

4. Расщепление информации.

Не все существующие методы обеспечения анонимности применены на практике. Те методы, которые реализованы, должны взаимодействовать со стеком протоколов TCP/IP. Это взаимодействие определяется тем, на каком уровне стека работает метод, анонимность какого протокола он обеспечивает. Существуют методы, работающие на сетевом уровне. Они транслируют IP пакеты, удаляя при этом из заголовка пакета всю секретную информацию, такую как IP адреса. Преимущество таких методов заключается в том, что они могут работать почти с любыми протоколами вышележащих уровней. Но с другой стороны, они могут потребовать модификации ядра операционной системы (так как IP-пакеты формируются в ядре), что делает их более сложными и менее портативными. Другие методы анонимности транслируют TCP трафик, причем обрабатывают этот трафик как поток, не разбивая на TCP сегменты. Эти методы не требуют вмешательства в ядро системы и могут работать со множеством приложений, которые поддерживают TCP или могут быть туннелированы через TCP. Третий класс методов — это методы, работающие на уровне приложений, чаще всего с протоколом HTTP. Это очень узконаправленные методы, но они также имеют свои преимущества. Так как вся идентификационная информация (например, cookie) из HTTP запросов удаляется, то количество передаваемых запросов сводится к минимуму и для их поддержания требуется минимум соединений.

1.3.1 Метод Mix-net

Основную роль в методе Mix-net играют специальные узлы, называемые миксами. Передача сообщений между отправителями и получателями происходит посредством миксов. Этот метод обеспечивает анонимность сеанса связи относительно внешнего локального пассивного адаптивного злоумышленника. Главная задача миксов – обеспечить битовую несвязываемость и перемешать входные сообщения, чтобы запутать злоумышленника.

Каждый микс имеет пару ключей – открытый и секретный. Отправитель сам выбирает через какие узлы-миксы будет передаваться его сообщение и формирует сообщение вида

$$E_{k_1}(E_{k_2}(\dots E_{k_n}(M, I_B)\dots, I_3),\ I_2), \tag{1.1}$$

где $E_{(\cdot)}$ – некоторый алгоритм асимметричного шифрования, $k_i,\ I_i\ i = 1, \dots n$ соответственно, открытые ключи и идентификаторы (адреса) узлов, через которые будет передаваться сообщение M, I_B – идентификатор получателя. Отправитель передает это сообщение узлу, который выбран им как первый узел маршрута. В текущих обозначениях этот узел имеет идентификатор I_1. Узел I_1 принимает зашифрованные сообщения от разных отправителей пока их количество не

достигнет некоторого n, затем расшифровывает их. Расшифровав сообщение (1.1), узлу I_1 становится известен следующий узел маршрута, это узел I_2, и сообщение $E_{k_2}(\dots E_{k_n}(M, I_B)\dots, I_3)$, предназначенное этому узлу. Расшифровав все n поступивших сообщений, узел I_1 отправляет извлеченные сообщения следующим узлам в лексикографическом или произвольном порядке.

В итоге, решение задачи секретной маршрутизации в Mix-net состоит в следующем. Только отправитель знает весь маршрут, так как он его формирует. Каждому промежуточному узлу маршрута, то есть каждому миксу, секретным образом сообщается минимум маршрутной информации, а именно в зашифрованном виде сообщается идентификатор следующего узла маршрута. Таким образом, никто в сети не обладает маршрутной информацией, кроме вовлеченных в передачу узлов. Задача обеспечения битовой несвязываемости решается с помощью шифрования. На каждом шаге сообщение расшифровывается, что приводит к тому, что битовые последовательности входного и выходного сообщений различны. К тому же входные сообщения накапливаются в миксе и отправляются не в том порядке в каком поступили, что препятствует атаке по временным характеристикам.

Метод Mix-net устойчив и к активному злоумышленнику при условии, что отправители сообщений поступающих в первый микс различны. Иначе, можно провести атаку [28], связанную с процессом накопления n сообщений в микс до того, как они будут обработаны и отправлены. С помощью этой атаки можно установить связь между входящими и выходящими сообщениями, отправляя в микс ложные сообщения не отличимые от легальных для всех кроме злоумышленника. Перехватив легальное сообщение M и сформировав $n-1$ ложных, злоумышленник на выходе микса сможет вычислить свои сообщения. Таким образом, станет известно выходящее сообщение соответствующее M. К глобальному злоумышленнику метод Mix-net не устойчив, если злоумышленник контролирует все миксы, составляющие маршрут сообщения, либо вступил в сговор с другими отправителями в количестве $n-1$, пересылающими свои сообщения по этим же миксам, то он может определить отправителя и получателя сообщения.

Идея Mix-net с разными вариациями, касающимися способов накопления входящих сообщений, реализована в методах [28–31].

Onion Routing [32] есть развитие идеи Mix-net для приложений требующих малых временных задержек. Борьба с задержками состоит в том, что сообщения не накапливаются в узлах: принятое сообщение после обработки сразу же передается далее. Задача секретной маршрутизации решается так же как и в Mix-net. Причем последовательные узлы выбранного маршрута не всегда соединены напрямую физически, чаще они соединены логически, то есть образуют оверлейную сеть. Onion Routing обеспечивает анонимность на уровне протокола TCP. В отличие от Mix-net, где отправитель для каждого передаваемого сообщения, для каждого микса должен выполнять операцию асимметричного шифрования, в Onion Routing асимметричное шифрование используется только при установлении соединения для передачи симметричного секретного

ключа.

Аналогично Mix-net, передача сообщений производится специальными узлами, которые в случае Onion Routing называются онион роутерами. Каждый онион роутер обладает секретным и открытым ключами. Отправитель выбирает последовательность онион роутеров, с помощью которых будет организован секретный канал. Затем генерирует пару секретных ключей k_{f_i}, k_{b_i} и криптографических функций f_i, f_i^{-1} для каждого онион роутера, (k_{f_i}, f_i) используется для передачи в прямом направлении, (k_{b_i}, f_i^{-1}) — в обратном.

При установлении секретного канала через онион роутеры $r_1,\ r_2, \dots r_n$ отправитель генерирует сообщение следующего вида

$$\begin{aligned} &E_1(f_1,\ k_{f_1},\ f_1^{-1},\ k_{b_1},\ r_2, \\ &\quad E_2(f_2, k_{f_2},\ f_2^{-1},\ k_{b_2},\ r_3, \\ &\qquad E_3(f_3,\ k_{f_3},\ f_3^{-1},\ k_{b_3},\ r_4, \dots E_n(f_n,\ k_{f_n},\ f_n^{-1},\ k_{b_n}, \emptyset) \dots))), \end{aligned} \tag{1.2}$$

где E_i – шифрование на открытом ключе онион роутера r_i. Каждый онион роутер расшифровывает сообщение, используя свой секретный ключ, и узнает предназначенные ему секретные ключи k_{f_i}, k_{b_i} и криптографические функции f_i, f_i^{-1}. Затем дополняет сообщение произвольными данными до первоначального размера, чтобы предотвратить отслеживание сообщения по размеру, и отправляет следующему узлу.

Передача данных производится уже с использованием симметричного шифрования. Отправитель формирует сообщение, последовательно зашифровывая его на симметричном ключе каждого онион роутера, входящего в маршрут сообщения. При передаче в прямом направлении (от отправителя) каждый онион роутер снимает один уровень шифрования, то есть расшифровывает полученное сообщение, при передаче в обратном направлении (к отправителю) — зашифровывает.

Усовершенствованная идея Onion Routing на практике реализована в системе Tor [33, 34]. Вместо формирования «луковицы» (1.2) для инициализации секретного канала отправитель последовательно устанавливает сеансовый секретный ключ с каждым онион роутером с помощью алгоритма Диффи-Хэлмана. Установив ключ с одним онион роутером, инициатор может использовать секретный канал через этот онион роутер, чтобы установить ключ со следующим онион роутером. После закрытия канала ключи удаляются. Благодаря этому, компрометация одного или нескольких онион роутеров не дает злоумышленнику возможности восстановить секретный ключ и расшифровать сообщение.

1.3.2 Метод DC-net

DC-net обеспечивает анонимность отправителя относительно внешнего глобального пассивного адаптивного злоумышленника. В основе метода лежит шифр Вернама, который является

совершенно секретным шифром.

Все пользователи $P_1, P_2, \ldots, P_n$ являются вершинами связного графа G. Граф G называется ключевым графом. В каждом раунде процесса передачи пользователи P_i и P_j, соединенные ребром в графе G, выбирают секретные ключи $k_{ij}(c),\ i, j, c \in \{1, 2, \ldots, n\},\ k_{ij}(c) = k_{ji}(c)$. Каждый пользователь P_i обладает вектором $W_i = \{W_i(1) = \oplus_{j=1}^{n} k_{ij}(1), W_i(2) = \oplus_{j=1}^{n} k_{ij}(2), \ldots, W_i(n) = \oplus_{j=1}^{n} k_{ij}(n)\}$.

Для того чтобы передать сообщение m_i, пользователь P_i выбирает произвольное c и зашифровывает m_i шифром Вернама с ключом $W_i(c)$, то есть вычисляет $W_i'(c) = m_i \oplus W_i(c)$, где $\oplus$ – сложение по модулю два. Полученный новый вектор W_i' отличается от W_i только в позиции c. Все W_i' передаются широковещательно. Тогда все пользователи сети могут вычислить вектор $W = \oplus_{i=1}^{n} W_i'$. Если остальные пользователи выбрали другие c, то вектор W состоит из сообщений пользователей. При условии, что ключи и номера слотов c храняться в секрете, невозможно выяснить кем было передано каждое из сообщений вектора W.

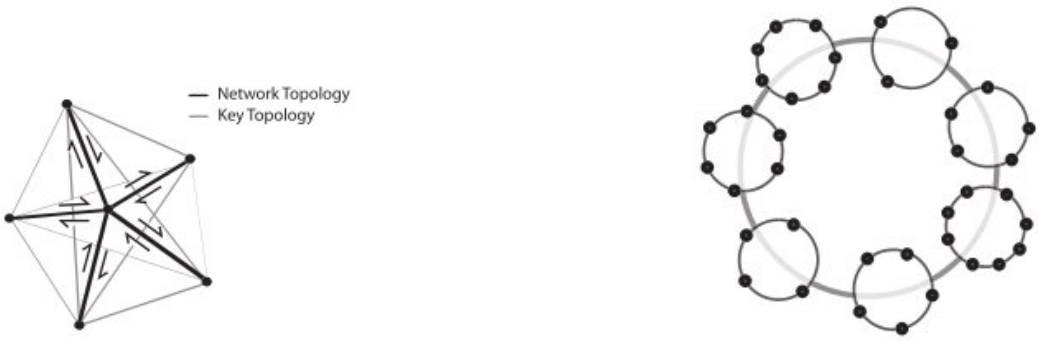
Таким образом, задача маршрутизации в DC-net вообще не стоит, так как сообщения передаются широковещательно. Благодаря широковещательной передаче, обеспечение несвязываемости тоже не требуется.

Серьезной проблемой DC-net являются коллизии. Если больше одного пользователя одновременно пытаются передать свое сообщение в одном слоте, то это приводит к тому, что ни одно сообщение не будет принято верно. Этим может воспользоваться злоумышленник: все время отправляя какие-то сообщения, он может разрушить работу всей системы.

Для борьбы с таким злоумышленником и с коллизиями в DC-net используется метод резервирования слота для передачи. Резервирование происходит таким образом. Пользователи P_i, P_j выбирают секретные ключи $k_{ij},\ i, j \in \{1, 2, \ldots, n\},\ k_{ij} = k_{ji}$ и передают сообщения, в которых отличен от нуля только один бит. Номер позиции этого бита есть номер слота, резервируемого для передачи. Тогда в суммарном сообщении $M = \oplus_i (m_i \oplus_j k_{ij})$ единичные биты обозначают зарезервированные слоты. Нулевые биты говорят о том, что эти слоты не будут использоваться. Пользователи, которые хотели передавать в этих слотах должны подождать следующего раунда передачи, чтобы выбрать другие слоты.

Метод DC-net не является стойким к активному злоумышленнику. Отсутствие возможности определить отправителя сообщения, предполагает наличие надежной широковещательной сети. Надежность здесь понимается в том смысле, что всякое сообщение переданное широковещательно достигает всех пользователей без изменения. Если это требование не выполнено, то можно провести атаку, позволяющую определить отправителя сообщения для топологии звезда, центральный узел которого контролируется злоумышленником [35].

К недостаткам DC-net можно отнести отсутствие масштабируемости и переиспользование пропускной способности. Для того, чтобы анонимно передать одно сообщение в сети должно



(а) Топология одной клики Herbivore (б) Глобальная топология Herbivore

Рис. 1.2: Топологии Herbivore [37]

быть передано $\Omega(n^2)$ сообщений.

В методе CliqueNet [36], основанном на идее DC-net, масштабируемость достигается путём организации пользователей в клики от 3 до 5 участников. Каждая клика имеет как минимум одну общую вершину с другими кликами, через которую передаются сообщения в другие клики. Эта идея была продолжена в Herbivore [37]. Пользователи формируют клики размером от k до $3k$, где k – заданное число, определяющее степень анонимности. Внутри клики пользователи связаны топологией звезда. Это оптимальная топология с точки зрения затрат пропускной способности: для анонимной передачи одного бита требуется передача $2(k-1)$ бит, что является минимальным числом бит, требующимся для анонимной передачи одного бита в DC-net сети, состоящей из k пользователей. Внутри клики пользователи взаимодействуют через центральный узел звезды (рис. 1.2а). Все сообщения передаются центральному узлу, а он затем широковещательно распространяет их между остальными узлами клики. Все клики организованы в кольцо (рис. 1.2б), с помощью которого осуществляется взаимодействие между ними.

Методы анонимности на основе DC-net являются наиболее стойкими, так как основаны на совершенно секретном шифре, но их сложность представляет собой главное препятствие практическому применению.

1.3.3 Методы анонимности на основе маршрутизации

Анонимность передачи сообщения может быть достигнута с помощью маршрутизации сообщения таким образом, чтобы его невозможно было отследить. В этом классе методов анонимности решением задачи секретной маршрутизации является динамическая вероятностная маршрутизация: маршрут строится в процессе передачи, причем каждый следующий узел выбирается случайно. Один из методов, воплощающих эту идею, Crowds [38], обеспечивает анонимность отправителя сообщения относительно активного локального адаптивного внешнего

злоумышленника и разработан для анонимной передачи веб запросов, т.е. работает на уровне приложений с протоколом HTTP.

Все пользователи сети Crowds образуют большую географически распределенную группу, называемую толпой, которая централизованно управляется сервером под названием блендер. Получатель сообщения, т.е. веб сервер, не способен определить отправителя сообщения, так как оно с равной вероятностью может быть отправлено любым членом группы. Новый пользователь проходит процесс инициализации, в ходе которого блендер сообщает ему секретные симметричные ключи для взаимодействия со всеми другими членами толпы. Оправляя запрос веб серверу, пользователь передает его произвольно выбранному члену толпы, предварительно зашифровав его на соответствующем секретном ключе. Получивший запрос узел расшифровывает его и решает отправить запрос следующему произвольному члену толпы или нужному веб серверу. Решение о передаче сообщения произвольному члену толпы принимается с вероятностью $p_f > \frac{1}{2}$. Сообщения между членами толпы передаются зашифрованными на секретном симметричном ключе, что обеспечивает битовую несвязываемость. При построении такого произвольного маршрута каждый следующий узел запоминает предыдущего с тем, чтобы получив ответ от веб сервера, передать его по тому же маршруту только в обратном направлении.

Анонимность отправителя достигается благодаря тому, что каждый член толпы, передающий сообщение, действует как прокси для предыдущего, то есть передаёт сообщение от имени предыдущего. Поэтому, перехватив сообщение в каком-либо узле маршрута, невозможно определить предыдущий ли узел является источником сообщения или любой из членов толпы.

Если в толпе имеется c злоумышленников и они могут сотрудничать, они не смогут определить отправителя сообщения, при условии, что $n \geq \frac{p_f}{p_f - \frac{1}{2}}(c+1)$, где n – количество членов толпы. Стойкость к взаимодействующим злоумышленникам снижается, если они могут обнаружить несколько маршрутов инициализированных одним и тем же пользователем, поэтому один однажды установленный маршрут используется для всех последующих запросов пользователя в течение определенного промежутка времени. Маршруты в системе Crowds меняются только при двух условиях: если на маршруте обнаружена неисправность, и по истечении срока действия. В первом случае до предшественника неисправного узла маршрут сохраняется, остальная его часть изменяется.

Установление срока действия маршрута связано с необходимостью присоединять к толпе новых пользователей. В случае появления в толпе новых пользователей все маршруты должны полностью меняться, иначе злоумышленник может связать вновь появившиеся маршруты с вновь появившимися пользователями. Процесс перестройки маршрутов всякий раз, как добавляется новый пользователь, подвержен атаке. Множество злоумышленников будут по очереди присоединяться к толпе, и каждый из них будет регистрировать кто является его предшественником при образовании маршрута. Некий пользователь P, который часто отправляет запросы,

то есть часто инициирует создание маршрута, будет чаще других появляться в маршруте и соответственно чаще регистрироваться злоумышленниками. Через некое количество итераций перестройки маршрутов станет очевидно, что P является инициатором маршрутов, т.е. отправителем запросов. Нужно по меньшей мере $\frac{8n}{c}\ln n$ итераций, чтобы P с большой вероятностью был зарегистрирован злоумышленниками как минимум в $4\ln n$ случаях [39]. Для предотвращения этой атаки новые пользователи добавляются все вместе и только в определённые моменты времени, а именно, во время истечения срока действия текущих маршрутов.

Схожий с Crowds метод Hordes [40], также предназначенный для обеспечения анонимности отправителя при передачи веб запросов, вносит одно существенное изменение, дающее дополнительные возможности для защиты отправителя — многоадресную рассылку. Способ построения маршрута в Hordes идентичен Crowds, но для передачи ответных сообщений отправителю используется не инвертированный маршрут, а многоадресная рассылка. Это позволяет тщательнее скрыть отправителя, поскольку технически сложно определить какие узлы сети являются членами некоторой группы многоадресной рассылки, но даже если это известно, невозможно выяснить какому узлу этой группы предназначено сообщение.

Формируя сообщение, отправитель указывает в нём к какой группе многоадресной рассылки он принадлежит и некое произвольное число. В ответном сообщении будет указано тоже самое число, что позволит отправителю определить, что это сообщение предназначено ему.

Так как ответное сообщение слышат все члены группы многоадресной рассылки, то злоумышленник, являющийся частью сети Hordes, может вычислить отправителя, используя корреляцию времен прохождения ответного сообщения и появления трафика на прямом маршруте. Так же как и в Crowds, в Hordes сообщения от отправителя шифруются каждым узлом маршрута на секретном ключе общим с последующим узлом маршрута. Таким образом, каждый узел маршрута знает к какой группе многоадресной рассылки принадлежит отправитель. Если какой-то узел маршрута является злоумышленником, он может прослушивать адрес группы рассылки и определить промежуток времени между ответным сообщением и новым сообщением от отправителя, которое будет передаваться по тому же маршруту, т.е. непременно пройдет через злоумышленника. Если этот промежуток времени мал, то с большой вероятностью отправителем является узел предшествующий злоумышленнику. Таким образом эти методы не являются стойкими к внутреннему злоумышленнику.

1.3.4 Расщепление информации

Идея расщепления информации с помощью метода SIS (Source Information Slicing) была впервые предложена в работе [41]. Здесь достигается анонимность как отправителя, так и получателя относительно внешнего локального пассивного адаптивного злоумышленника. Идея расщепления информации решает задачу маршрутизации также как Onion Routing: отправи-

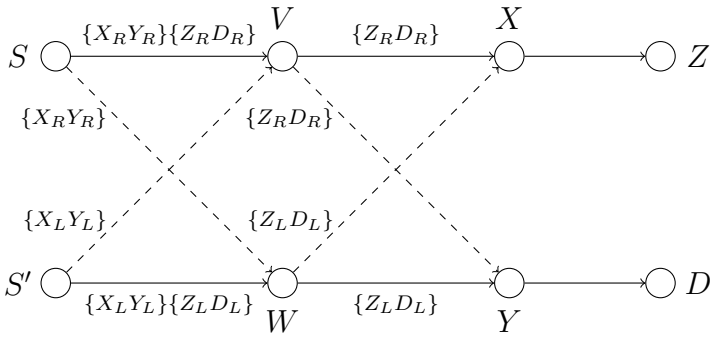


Рис. 1.3: Схема передачи метода SIS

тель самостоятельно выбирает узлы, которые войдут в состав маршрута и секретно передает каждому узлу его маршрутную информацию. Предполагается, что отправитель имеет более одного IP адреса. Дополнительные адреса образуют псевдоисточники сообщений. Основной источник сообщения может установить секретный канал со всеми псевдоисточниками. Расщепление информации позволяет передать сообщение секретно без использования шифрования. Если секретно передавать сообщения, содержащие адреса следующих узлов, то можно построить маршрут для анонимной передачи. Рассмотрим работу метода на примере (рис. 1.3). Части информации должны передаваться по непересекающимся маршрутам. Для того чтобы образовать нужное количество непересекающихся маршрутов строится граф передачи. Отправитель S имеет псевдоисточник S'. Отправитель строит граф передачи, выбирая некоторое количество промежуточных узлов и организуя их каскадно, таким образом чтобы в каждом каскаде было по два узла. Узлы соседних каскадов связаны между собой. Чтобы анонимно отправить сообщение, отправитель должен сообщить узлам V и W адреса следующих за ними узлов маршрута, то есть X и Y, а узлам X и Y надо сообщить адреса следующих за ними узлов Z и D. Для этого он делит каждый из адресов X, Y, Z, D на две части X_lX_r, Y_lY_r, Z_lZ_r и D_lD_r соответственно (индексы l и r обозначают левую и правую части) и получает части сообщения

$$\begin{pmatrix} X_L \\ X_R \end{pmatrix} = \mathbf{A} \begin{pmatrix} X_l \\ X_r \end{pmatrix}, \begin{pmatrix} Y_L \\ Y_R \end{pmatrix} = \mathbf{A} \begin{pmatrix} Y_l \\ Y_r \end{pmatrix}, \begin{pmatrix} Z_L \\ Z_R \end{pmatrix} = \mathbf{A} \begin{pmatrix} Z_l \\ Z_r \end{pmatrix}, \begin{pmatrix} \text{Боб}_L \\ \text{Боб}_R \end{pmatrix} = \mathbf{A} \begin{pmatrix} D_l \\ D_r \end{pmatrix},$$

где $\mathbf{A}$ – произвольная обратимая матрица размером 2×2. Части сообщения X представляют собой пары X_L, A_1 и X_R, A_2 (A_1 и A_2 – первая и вторая строки матрицы $\mathbf{A}$ соответственно). Аналогично задаются части других сообщений. Узел V получает от S сообщение $\{X_R, Y_R\}\{Z_R, D_R\}$ (предполагается, что соответствующие строки матрицы $\mathbf{A}$ в этом сообщении также передаются), а от S' сообщение $\{X_L, Y_L\}$. Получив все части, он может вычислить адреса следующих за ним узлов X и Y:

$$\begin{pmatrix} X_l & Y_l \\ X_r & Y_r \end{pmatrix} = \mathbf{A}^{-1} \begin{pmatrix} X_L & Y_L \\ X_R & Y_R \end{pmatrix}.$$

Теперь узел V может отправить оставшуюся у него часть сообщения $\{Z_R, D_R\}$, дополнив её произвольными битами, узлам X и Y. Узел W аналогичным с V образом определяет адреса узлов X и Y. После этого он отправит им сообщение $\{Z_L, D_L\}$, дополненное произвольными битами. Узлы X и Y, получив от узлов V и W соответствующие сообщения, будут иметь достаточно информации, чтобы определить адреса узлов Z и D. Узлы X и Y, также как узлы V и W, не могут определить кто является источником сообщений и кто получателем. Теперь маршруты для передачи сообщений узлу D определены. Отправитель может расщеплять свои сообщения на две части и отправлять D по непересекающимся путям графа передачи. Если злоумышленник может контролировать один из промежуточных узлов, то он обладает частью информации о маршруте. Контролирование одного узла на каждом из маршрутов не может привести к компрометации отправителя, но может существенно уменьшить множество возможных получателей. Вернёмся к примеру на рисунке 1.3. Если злоумышленник контролирует узлы W и X, то он может сделать вывод о том, что получателем является либо Z, либо D. Для того чтобы восстановить сообщение, содержащее маршрутную информацию, достаточно контролировать по одному узлу на каждом из путей графа передачи.

Требование к отправителю иметь несколько IP адресов является неудобным и порой трудноосуществимым на практике. Способ построения графа для анонимной передачи не является хорошо масштабируемым.

Другой метод расщепления информации AC-ITNC предложен в [42]. Этот метод предназначен для формирования маршрутов для анонимной передачи. Передача сообщений производится с помощью Onion Routing и симметричного шифрования. Метод $AC - ITNC$ является более сложным, так как для формирования маршрута длины L требуется построить L различных графов передачи.

Подводя итог проведенному анализу, можно заключить, что методы из класса DC-net (DC-net, CliqueNet, Herbivore) слишком сложны в использовании, так же, как и методы, основанные на расщеплении информации (SIS и AC-ITNC), процедура построения графа передачи которых является трудоемкой и плохо масштабируемой. Главный недостаток Crowds и Herbivore состоит в вероятностной маршрутизации, которая может приводить к излишнему использованию пропускной способности, так как пакеты данных некоторое время блуждают по сети. Идея Onion Routing реализована на практике в виде анонимной сети Tor, что свидетельствует о её практической пользе. Но, с другой стороны, Onion Routing представляет криптографический подход, следовательно, требует выработки и распределения секретных ключей, что усложняет построенную сеть.

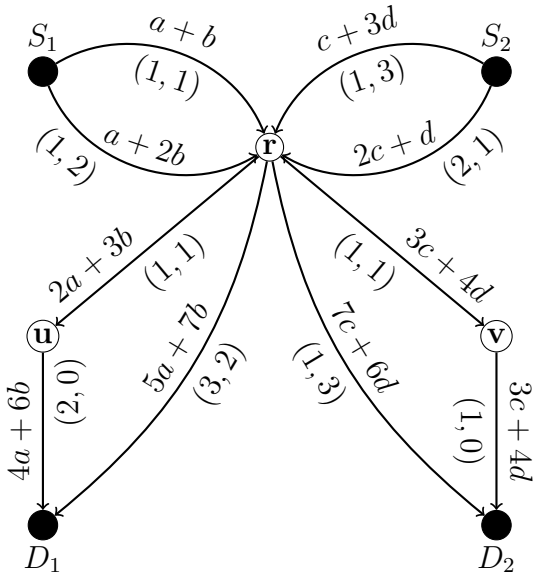


Рис. 1.4: Пример когерентного сетевого кодирования

1.4 Методы обеспечения анонимности в сетевом кодировании

Подробнее сетевое кодирование рассматривается в главе 2. Здесь приведем пример сетевого кодирования, который иллюстрирует возможности злоумышленника для компрометации анонимности, а также приведем сравнительный анализ методов анонимности для сетевого кодирования на основе работы [13].

В линейном сетевом кодировании промежуточные узлы составляют линейные комбинации поступивших пакетов данных. Коэффициенты линейных комбинаций заданы. По каждому соединению передаются линейные комбинации пакетов с коэффициентами, принадлежащими именно этому соединению. Эти коэффициенты формируют вектор, называемый *кодирующим*. Каждое соединение обладает собственным кодирующим вектором. Такой способ получил название *когерентного* сетевого кодирования. Другой способ задания кодирующих векторов состоит в том, что каждый передающий узел самостоятельно произвольным образом выбирает кодирующие векторы для каждого набора входящих пакетов. Чтобы обеспечить декодирование сообщения на узле получателя, кодирующие векторы в этом случае передаются вместе с пакетами. Линейное преобразование на промежуточных узлах с помощью выбранных ими кодирующих векторов применяется в этом случае не только к поступившим пакетам, но и к кодирующим векторам, поступившим с этими пакетами. Этот способ сетевого кодирования называется *некогерентным* или *случайным*. Рассмотрим пример сетевого кодирования с двумя источниками и двумя получателями, представленный на рисунке 1.4. Узел S_1 передаёт два пакета a и b узлу

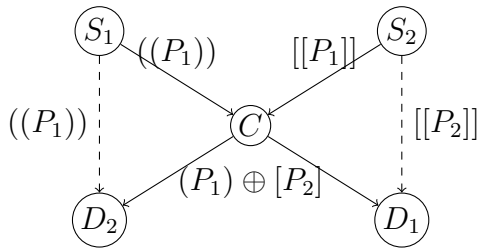


Рис. 1.5: Схема работы метода ANOC

D_1, а узел S_2 – пакеты c и d узлу D_2. Соответствующие соединениям кодирующие векторы и передаваемые по ним пакеты указаны на рисунке. Злоумышленник может прослушать все входные соединения узла r. После этого он будет обладать пакетами $a + b,\ a + 2b$, отправленными узлом S_1, и пакетами $c + 3d,\ 2c + d$, отправленными узлом S_2. Прослушав соединение $r \to D_1$, злоумышленник получит пакет $5a+7b$. Кодирующий вектор соединения $r \to D_1$ равен $(3, 2)$. Для того чтобы определить пакеты какого источника передаются по соединению $r \to D_1$, злоумышленнику необходимо просто сделать проверку линейной комбинации каждой пары поступивших пакетов в r пакетов с коэффициентами 3 и 2 с тем пакетом, что передается по соединению $r \to D_1$. Таким образом он определит, что

$$3(a + b) + 2(a + 2b) = 5a + 7b,$$
$$3(c + 3d) + 2(2c + d) \neq 5a + 7b.$$

Это дает ему возможность сделать вывод, что по $r \to D_1$ передаются пакеты от S_1, то есть D_1 – это адресат отправителя S_1.

Следовательно, линейная зависимость между пакетами, поступающими в узел и отправляемыми им, может использоваться для выявления маршрута сообщения.

Один из способов обеспечения анонимности в сетях с сетевым кодированием — это адаптирование успешных методов анонимности традиционного способа передачи данных к сетевому кодированию. Одним из таких методов является ANOC [43]. Этот метод обеспечивает анонимность сеанса связи для беспроводных меш сетей. Основу этого метода составляет Onion Routing. Поскольку перемешивание пакетов разных потоков данных, свойственное для сетевого кодирования, не позволяет корректно осуществлять шифрование/расшифрование, требуется введение дополнительных операций, которые позволят разрешить этот конфликт. В ANOC этими дополнительными операциями являются распределение сессионных ключей для симметричного шифрования и дополнительное расшифрование. Рассмотрим пример схемы передачи представленный на рисунке 1.5. Каждый узел имеет открытый ключ pk, к примеру pk_C — открытый ключ, принадлежащий узлу C. Узлу S_1 необходимо передать секретные сессионные ключи k_C^1 и $k_{D_1}^1$ узлам C и D_1 соответственно. Для этого S_1 отправляет C сообщение $E_{pk_C}(E_{pk_{D_1}}(k_{D_1}^1), k_C^1, I_{D_1})$, где $E_{(\cdot)}(\cdot)$ – функция асимметричного шифрования. Расшифровав это сообщение, узел C из-

влекает свой секретный ключ k_C^1. Идентификатор I_{D_1} указывает узлу C на то, что следующим узлом в маршруте будет D_1. Узел C отправит сообщение $E_{pk_{D_1}}(k_{D_1}^1)$ узлу D_1, который извлечёт свой секретный ключ $k_{D_1}^1$. Аналогичным образом, S_2 установит секретные сессионные ключи k_C^2 и $k_{D_2}^2$ с узлами C и D_2 соответственно. Теперь, если узел S_1 хочет передать сообщение m_1 узлу D_1, то он передает сообщение $((P_1)) = E_{k_C^1}(E_{k_{D_1}^1}(m_1))$, которое будет получено узлом C, а также узлом D_2, который прослушивает эфир. Чтобы передать сообщение m_2 узлу D_2, узел S_2 отправит сообщение $[[P_2]] = E_{k_C^2}(E_{k_{D_2}^2}(m_2))$, которое получат узлы C и D_1. Узел C снимает один уровень шифрования с полученных сообщений $((P_1)), [[P_2]]$ и отправляет узлам D_1 и D_2 сообщение вида $(P_1) \oplus [P_2] = E_{k_{D_1}^1}(m_1) \oplus E_{k_{D_2}^2}(m_2)$. Узел D_1, имея сообщения $[[P_2]]$ и $(P_1) \oplus [P_2]$, не сможет получить m_1. Аналогично, D_2 из сообщений $((P_1))$ и $(P_1) \oplus [P_2]$ не получит m_2. Узел C широковещательно отправляет свои секретные ключи k_C^1, k_C^2 соседним узлам. Узел D_1 с помощью ключа k_C^2 из сообщения $[[P_2]] = E_{k_C^2}(E_{k_{D_2}^2}(m_2))$ извлекает $[P_2] = E_{k_{D_2}^2}(m_2)$. Сложив по модулю два сообщение $(P_1) \oplus [P_2]$ с сообщением $[P_2]$, он получит $(P_1) = E_{k_{D_1}^1}(m_1)$. Расшифрование этого сообщения на узле D_1 даст сообщение m_1. Аналогично узел D_2 получает сообщение m_2.

При использовании случайного сетевого кодирования основные усилия направлены на защиту кодирующего вектора. При случайном сетевом кодировании линейное преобразование применяется не только к поступившим пакетам, но и к поступившим с пакетами кодирующим векторам. Следовательно, выходящие и входящие кодирующие векторы линейно зависимы. Тогда выявлять маршрут сообщения можно не с помощью самого сообщения, а с помощью кодирующих векторов, что может быть проще, так как кодирующие векторы занимают меньше памяти.

В методе ALNCode [44] каждый промежуточный узел строит кодирующий вектор определённым способом. Новый кодирующий вектор должен принадлежать пространству, базис которого является общим для пространств кодирующих векторов всех информационных потоков, входящих в этот узел. Пассивный внешний злоумышленник в этом случае не может найти связь между сообщениями, входящими в узел и выходящими из узла. Метод ALNCode обеспечивает анонимность сеанса связи. Каждый промежуточный узел собирает закодированные сообщения, принадлежащие одному информационному потоку, поступившие в течение заданного количества временных слотов. Пусть V_i – множество кодирующих векторов сообщений потока i, а $V' = \cup_{l \neq i} V_l$ – множество кодирующих векторов сообщений других потоков, поступающих в этот узел. Новый кодирующий вектор v_i сообщений из потока i является линейной комбинацией вектора из пространства $L(V_i)$ и вектора из пространства $L(V_i) \cap L(V')$, где $L(\cdot)$ – линейная оболочка множества. Отследить сообщение с кодирующим вектором v_i трудно, поскольку вектор v_i связан с кодирующими векторами всех потоков, поступающих в промежуточный узел. На рисунке 1.6 показано три потока $s_i \to d_i,\ i \in \{1, 2, 3\}$, которые проходят через общий узел k. В узел k поступает по два закодированных сообщения каждого потока с кодирующими векторами

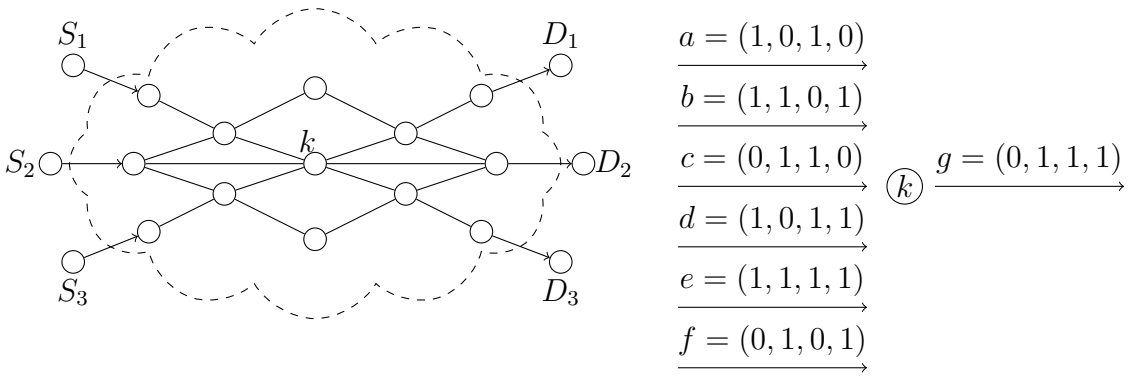


Рис. 1.6: Пример использования метода *ALNCode* [44]

$a = (1, 0, 1, 0),\ b = (1, 1, 0, 1)$ от первого потока, $c = (0, 1, 1, 0),\ d = (1, 0, 1, 1)$ от второго потока, $e = (1, 1, 1, 1),\ f = (0, 1, 0, 1)$ от третьего потока. Новый кодирующий вектор для первого потока может быть получен как $g = a + b = (0, 1, 1, 1)$. Вектор $(0, 1, 1, 1)$ также может быть получен или как $a + c + d$, или как $b + e + f$, или как $c + d + e + f$. Сложность операции установления связи между выходящим и входящими кодирующими векторами экспоненциально растет с увеличением количества входящих в узел кодирующих векторов. Таким образом, компрометация корреспондентов является вычислительно трудной задачей.

Другой способ защиты кодирующего вектора — это шифрование. Шифрование на ключе, общем для отправителя и получателя, невозможно, поскольку промежуточные узлы могут перемешивать сообщения, и на стороне получателя нельзя будет правильно восстановить сообщение.

В работе [45] предлагается использовать гомоморфное шифрование для защиты кодирующего вектора. Промежуточные узлы при этом могут осуществлять линейные операции над кодирующими векторами, не расшифровывая их. Этот метод также обеспечивает анонимность сеанса связи. Отправитель кодирует сообщения $\{m_1, \ldots, m_h\}$ с помощью векторов $\{v_1, \ldots, v_h\}$ в виде $m'_i = \sum_{j=1}^{h} m_j v_{ij}$. Затем он шифрует кодирующие векторы в виде $c_i = E_{pk}(v_i),\ 1 \le i \le h$, где pk – открытый ключ получателя, $E(\cdot)$ – функция гомоморфного шифрования, обладающая свойством $E(m_1)E(m_2) = E(m_1 + m_2)$. Получив сообщения $\{c_i, m'_i\},\ 1 \le i \le h$, промежуточный узел выбирает произвольный вектор $l = (l_1, \ldots, l_h)$ и кодирует с его помощью поступившие сообщения в виде $m'' = \sum_i l_i m'_i$. Кодирующий вектор имеет вид $g = \sum_i l_i v_i$. Гомоморфное шифрование позволяет вычислить $E_{pk}(g)$, не зная v_i, а зная только $E_{pk}(v_i) = c_i$. Это можно сделать следующим образом $w = E_{pk}(g) = E_{pk}(\sum_{i=1}^{h} l_i v_i) = \prod_{i=1}^{h} E_{pk}(l_i v_i) = \prod_{i=1}^{h} E_{pk}^{l_i}(v_i) = \prod_{i=1}^{h} c_i^{l_i}$. При восстановлении сообщения на стороне получателя предварительно должна быть выполнена операция расшифрования $g = D_{sk}(w)$ с помощью секретного ключа получателя. Наличие шифрования не позволяет злоумышленнику найти связь между сообщениями, входящими в узел и выходящими из узла. Поэтому невозможно отследить путь передачи сообщения.

Имеется похожий метод, называемый P-code [46]. Он предполагает использование перестановочного шифра, удовлетворяющего следующим условиям: $E_k(m+n) = E_k(m) + E_k(n)$ и $E_k(tm) = tE_k(m)$. Использование гомоморфного шифрования не требует производить операции шифрования/расшифрования на каждом промежуточном узле.

Подводя итог проведенному анализу, можно отметить, что адаптирование успешной в традиционных сетях идеи Onion Routing к сетевому кодированию в виде метода ANOC не является удачным так, как ведет к усложнению процесса передачи и увеличению задержек из-за введения двух дополнительных операций. Методы, использующие криптографический подход, обладают его недостатками. ALNCode – единственный метод, использующий суть сетевого кодирования. Но он не может быть применен для когерентного сетевого кодирования, где кодирующие векторы заданы, и для аналогового сетевого кодирования, где кодирующие векторы не могут произвольным образом выбираться передающим узлом, а зависят от канала (пункт 3.2).

1.5 Численные характеристики анонимности

В определениях анонимности говорится, что злоумышленник не может определить что-либо достоверно. Это значит, что анонимность можно количественно измерить. Рассмотрим существующие количественные характеристики анонимности. Эти количественные характеристики можно разделить на несколько классов по трем признакам (Таб. 1.1). Первый признак отвечает за глобальность и локальность характеристики. Глобальная характеристика определяет анонимность системы передачи в целом. Под системой передачи понимается совокупность множеств получателей, отправителей и сообщений, которыми они могут обмениваться. Тогда глобальная характеристика определяет какой уровень анонимности обеспечивается, например, для всех получателей системы или для всех отправителей. Локальная характеристика определяется для каждого конкретного объекта, будь то получатель, отправитель или сообщение. Второй признак – тип анонимности. Количественную характеристику можно ввести для анонимности отправителя, анонимности получателя или анонимности сеанса связи. Последний признак отвечает за подход к определению характеристики. Можно выделить два подхода – вероятностный и комбинаторный. Вероятностный подход основан на том, что после проведения атаки злоумышленник обладает некоторым распределением вероятностей, которое описывает предмет атаки. Например, для каждого из возможных отправителей злоумышленник может определить вероятность того, что этот отправитель действительно является источником некоторого сообщения. При комбинаторном подходе уровень анонимности определяется самой системой передачи, а не распределением вероятностей, которое может получить злоумышленник, но может быть обобщен и на случай, когда злоумышленник обладает распределением вероятностей.

Способ определения \ Тип анонимности			Отправитель, получатель	Сеанс связи
Вероятностный	Вероятность		$1 - p_i$ [47] $p_{ij} \leq \Theta$ [48]	
	Энтропия	Энтропия Шеннона	$\frac{H(X)}{H_M}$ [49] $H(X)$ [50]	
		Энтропия Реньи	$H_\alpha(X)$ [51]	
	Взаимная информация			$1 - \frac{I((S,R)_a;(S,R)_s)}{\log_2 mn}$ [53]
	Расстояние Кульбака-Лейблера		$\max_f D(P, f(P)) \leq \alpha$ [52]	
Комбинаторный			$\log_2 N$ [56]	$\frac{\log_2 \mathrm{per}(A)}{\log_2 n!}$ [54], [55]

Таблица 1.1: Численные характеристики анонимности, классифицированные по способу их определения и типу анонимности, для которого они предназначены

Характеристики на основе вероятности для анонимности отправителя или получателя были предложены в работах [47, 48]. Степень анонимности в работе [47] определена в виде $1 - p_i$, где p_i – это определенная злоумышленником вероятность того, что некоторый узел i является отправителем (получателем) сообщения. Эту характеристику нельзя использовать отдельно от конкретной системы передачи. Например, в системе передачи состоящей из трех узлов, которые могут обмениваться сообщениями друг с другом, степень анонимности одного из узлов, назовем его r_1, равна $\frac{3}{4}$, а для двух других одинакова и равна $\frac{5}{8}$. В другой системе, состоящей из десяти узлов, узел r_2 имеет степень анонимности $\frac{3}{4}$, а остальные – $\frac{11}{12}$. Несмотря на то, что узлы r_1 и r_2 имеют одинаковую степень анонимности, они не являются одинаково защищенными. Узел r_1 внутри своей системы передачи является более анонимным, чем узел r_2 внутри своей системы, так как все остальные узлы во второй системе имеют большую степень анонимности. Степень анонимности является локальной характеристикой. Она вычисляется для каждого узла и определяет защищенность отдельного узла. В противоположность этому характеристика, предложенная в [48], является глобальной. Она определяет защищенность всех отправителей

или всех получателей. Система передачи обеспечивает анонимность отправителей с параметром Θ, если злоумышленник не может определить отправителя сообщения, принятого конкретным получателем, с вероятностью, превышающей Θ, то есть если для любого отправителя i и любого сообщения j выполняется $p_{ij} \leq \Theta$. Аналогично, система передачи обеспечивает анонимность получателей с параметром Ω, если злоумышленник не может определить получателя сообщения, отправленного конкретным отправителем, с вероятностью, превышающей Ω. Эта характеристика рассматривает анонимность как бинарное свойство:система обеспечивает анонимность, если все вероятности не превосходят порогового значения и не обеспечивает в противном случае.

Характеристики, использующие энтропию, определяют количество дополнительной информации нужно злоумышленнику, чтобы точно установить отправителя (получателя) сообщения. Характеристика, предложенная в работе [49], является глобальной. Она определяет анонимность всех получателей системы и выражается в виде

$$1 - \frac{H_M - H(X)}{H_M} = \frac{H(X)}{H_M},$$

где H_M определяет максимальную энтропию системы $H_M = \log_2 N$, а $H(X)$ определяет энтропию системы после проведенной злоумышленником атаки. Для каждого из N возможных отправителей злоумышленник вычисляет вероятность p_i того, что этот потенциальный отправитель действительно отправил конкретное сообщение. Тогда

$$H(X) = -\sum_{i=1}^{N} p_i \log_2 p_i.$$

Ненормированная на максимальную энтропию величина $H(X)$ была предложена в качестве характеристики анонимности под названием эффективный размер множества анонимности в работе [50]. Эта характеристика связана с пороговой характеристикой [48] следующим образом: $H(X) \geq -\log_2 \Theta$. В качестве обобщения характеристик шенноновской энтропии можно использовать энтропию Реньи [51]

$$H_\alpha(X) = \frac{1}{1-\alpha} \sum_i p_i^\alpha,$$

что позволяет переходить от характеристики в худшем случае к характеристике лучшего случая, то есть от минимальной энтропии к максимальной, варьируя параметр α. Все перечисленные выше характеристики, основанные на энтропии, страдают от недостатка, связанного с чувствительностью энтропии к выбросам. Получатель с очень маленькой вероятностью может вносить большой вклад в энтропию. Высокая энтропия говорит о высоком уровне защищённости всех получателей системы, но в тоже время необъективно отражает защищенность каждого отдельного получателя. Имеется ещё одна глобальная характеристика, которая основана на расстоянии Кульбака-Лейблера [52]. Система передачи может быть описана процессом P, заданным на некотором множестве анонимных действий A. Тогда система называется α-анонимной, если

расстояние Кульбака-Лейблера между распределением вероятностей, описывающим процесс P, и распределением вероятностей, описывающим некоторую перестановку на множестве A, не превосходит α, то есть

$$\forall f \in F_A \;\; D(P, f(P)) \leq \alpha,$$

где F_A обозначает все возможные перестановки на множестве A. Рассмотрим пример. Пусть имеется сеть, в которой два узла S_1 и S_2 могут отправлять сообщения узлу R. Злоумышленник пытается определить какой именно узел отправил сообщение. Множество A состоит из двух действий $A = \{\text{отправил } S_1, \text{отправил } S_2\}$. Система описывается процессом

$$P = u_p.(R \text{ получил сообщение от } S_1) + u_{1-p}.(R \text{ получил сообщение от } S_2),$$

где запись $u_p.(R$ получил сообщение от $S_1)$ означает, что процесс совершил действие u с вероятностью p и продолжился далее как процесс (R получил сообщение от S_1), а знак «+» означает «или», то есть процесс развивается либо как первое слагаемое, либо как второе. На заданном множестве A возможна только одна перестановка, которая задаёт процесс

$$f(P) = u_{1-p}.(R \text{ получил сообщение от } S_1) + u_p.(R \text{ получил сообщение от } S_2).$$

Тогда

$$D(P, f(P)) = p \log \frac{p}{1-p} + (1-p) \log \frac{1-p}{p}.$$

Максимум достигается при $p = \frac{1}{2}$, и злоумышленник не может определить, кто именно отправил сообщение.

Пусть случайная величина $(S, R)_a$ представляет собой истинную пару отправитель–получатель, а случайная величина $(S, R)_s$ – предполагаемую пару. Если злоумышленник может предсказывать пару, то величины $(S, R)_a$ и $(S, R)_s$ будут зависимыми. В работе [53] предлагается характеристика анонимности сеанса связи вида

$$1 - \frac{I((S, R)_a; (S, R)_s)}{\log_2 mn},$$

где $I((S, R)_a; (S, R)_s)$ – взаимная информация между величинами $(S, R)_a$ и $(S, R)_s$, m – количество отправителей, n – количество получателей.

Комбинаторный подход был предложен для системы Mix-net. Принцип комбинаторного подхода был впервые рассмотрен в работе [54] и далее развит в работе [55]. Рассматривается система передачи, состоящая из множества отправителей, множества получателей и анонимной сети, состоящей из множества миксов, посредством которой происходит передача между отправителями и получателями. Известны пары вида (сообщение, время поступления в анонимную сеть), обозначим их (m_i, s_i), и пары вида (сообщение, время выхода из анонимной сети), обозначим их (m_j, t_j). Количество этих пар совпадает и равно n. Задача злоумышленника заключается

в том, чтобы построить соответствие между парами (m_i, s_i) и (m_j, t_j), что позволит ему скомпрометировать анонимность сеанса связи. Можно построить двудольный граф, где множество вершин есть множество всех s_i и t_j, а множество ребер формируется следующим образом. Если разница $t_j - s_i$ лежит в некотором заданном интервале, то имеется ребро между s_i и t_j, иначе ребра нет. Такой граф будет определять, в какие сообщения на выходе из анонимной сети могло перейти конкретное входное сообщение. Защищённость сообщений определяется количеством совершенных паросочетаний. Если граф полный, то система передачи обеспечивает максимальную анонимность для всех сообщений. Количество совершенных паросочетаний графа задаётся перманентом матрицы связности. Построив матрицу связности $\mathbf{A}$ этого графа, можно определить характеристику анонимности в виде

$$\begin{cases} \frac{\log_2 \operatorname{per}(\mathbf{A})}{\log_2 n!}, \ n > 1, \\ 0, \ n = 1, \end{cases}$$

где $\operatorname{per}(\mathbf{A})$ – перманент матрицы $\mathbf{A}$. Если злоумышленник может построить распределение вероятностей, описывающее связь между входами и выходами, тогда матрица $\mathbf{A}$ будет дважды стохастической матрицей, а не матрицей связности. Каждый элемент a_{ij} задает вероятность того, что входное сообщение i перешло в выходное сообщение j. В этом случае характеристику нужно нормировать, используя минимум перманента дважды стохастической матрицы, который равен $\frac{n!}{n^n}$. Она будет выражаться в виде

$$\left\{ \frac{\log_2 \operatorname{per}(\mathbf{A})}{\log_2(\frac{n!}{n^n})}, \ n > 1, 0, \ n = 1. \right.$$

К недостаткам этой характеристики можно отнести её специфичность, так как она предложена для методов анонимности, основанных на идее об использовании миксов. Кроме того, что вычисление перманента матрицы в общем случае является NP-полной задачей. Характеристику, предложенную в работе [56], также можно отнести к комбинаторному подходу, так как она не принимает во внимание наличие злоумышленника, который может получить некоторую информацию. Степень анонимности определяется только размером сети передачи как $\log_2 N$, где N – количество возможных отправителей (получателей). Это глобальная характеристика, которая описывает анонимность всех отправителей или всех получателей.

Так как атаки из класса анализа трафика обычно приводят к тому, что злоумышленник обладает некоторым распределением вероятностей, то вероятностные характеристики на основе энтропии или взаимной информации оказываются более практически применимыми по сравнению с комбинаторными характеристиками, которые, во-первых, не принимают во внимание вероятностной информации злоумышленника, а во-вторых, просто сложны в использовании, равно как и характеристика на основе расстояния Кульбака-Лейблера.

1.6 Совершенная несвязываемость

Характеристика для количественной оценки анонимности зависит от типа анонимности. Из анализа 1.5 ясно, что единственной вероятностной характеристикой для анонимности сеанса связи является степень анонимности $D = 1 - \frac{I((S;R)_a;(S;R)_s)}{\log_2 mn}$. С помощью этой характеристики можно опосредованно оценивать несвязываемость сообщений, если злоумышленник предсказывает пару отправитель-получатель $(S;R)_s$ на основе прослушивания входных и выходных сообщений узлов и установления между ними связей. Но нормировочный коэффициент $\log_2 mn$ отсылает к утверждению, состоящему в том, что чем больше множество анонимности, то есть чем больше количество отправителей m и количество получателей n, тем лучше узлы защищены, что стало неверным с развитием атак анализа трафика.

Для численной оценки несвязываемости можно использовать характеристики, которые используются для оценки секретности. Пусть отправитель хочет передать сообщение, описываемое случайной величиной M, заданной на множестве $\mathbb{M}$. Пусть информация, которой обладает злоумышленник, описывается случайным вектором W длины n. Выделяют шесть вероятностных характеристик секретности.

1. Взаимная информация $I(M;W)$.
2. Статистическое расстояние $\Delta(P(MW), P(M)P(W))$, где статистическое расстояние между случайными величинами X и X', заданными на множестве $\mathbb{X}$ определяется в виде $\Delta(P(X), P(X')) = \sum\limits_{x \in \mathbb{X}} |P(X = x) - P(X' = x)|$.
3. Не усреднённая взаимная информация $i(M;W) = \log_2 \frac{P(MW)}{P(M)P(W)}$.
4. $\frac{I(M;W)}{n}$.
5. $\frac{\Delta(P(MW),P(M)P(W))}{n}$.
6. $\frac{i(M;W)}{n}$.

Введём понятие отношения между характеристиками.

Определение 1.5 ([57]). *Считаем, что характеристика $\delta_n^{(1)}$ строже характеристики $\delta_n^{(2)}$, $\delta_n^{12)} \succeq \delta_n^{(2)}$, если из схождения по вероятности к нулю характеристики $\delta_n^{(1)}$ следует схождение по вероятности к нулю характеристики $\delta_n^{(2)}$, то есть если*

$$\forall \epsilon > 0 \lim_{n \to \infty} P(|\delta_n^{(1)}| > \epsilon) = 0 \Rightarrow \lim_{n \to \infty} P(|\delta_n^{(2)}| > \epsilon) = 0.$$

Первая характеристика задаёт понятие *совершенной* и *строгой* секретности. Понятие совершенной секретности было предложено Шенноном [58].

Определение 1.6. *Сообщение M передается совершенно секретно, если $I(M;W)=0$.*

Определение 1.7. *Сообщение M называется секретным в строгом смысле, если*

$$\lim_{n\to\infty} I(M;W)=0. \tag{1.3}$$

Четвертая характеристика задает понятие *слабой* секретности.

Определение 1.8. *Сообщение M называется секретным в слабом смысле, если*

$$\lim_{n\to\infty} \frac{I(M;W)}{n}=0. \tag{1.4}$$

Можно установить следующее соотношение между вышеперечисленными характеристиками ([57])

$$I(M;W)\succeq\Delta(P(MW),P(M)P(W))\succeq i(M;W)\succeq\frac{I(M;W)}{n}\succeq\frac{\Delta(P(MW),P(M)P(W))}{n}\succeq\frac{i(M;W)}{n}.$$

Таким образом, взаимная информация является наиболее строгой вероятностной характеристикой. Она также является простым, понятным и хорошо интерпретируемым способом оценки эффективности атак злоумышленника, так как большинство атак злоумышленника приводит к тому, что он находит распределение вероятностей, описывающее интересующие его объекты.

С помощью взаимной информации можно непосредственно оценивать несвязываемость сообщений. Обозначим через f некоторый алгоритм, который преобразовывает сообщение M в сообщение $X\in\mathbb{X}$ для его последующей передачи, $f:\mathbb{M}\to\mathbb{X}$. В общем случае функция f не является детерминированной. Пусть X^{in} является входным сообщением некоторого промежуточного узла. Пусть выходное сообщение этого промежуточного узла, соответствующее сообщению X^{in}, описывается случайной величиной X^{out}. По аналогии с совершенной секретностью определим *совершенную несвязываемость* сообщений.

Определение 1.9. *Сообщения X^{in} и X^{out} называются совершенно несвязываемыми, если выполняется $I(X^{in};X^{out}|M)=0$.*

Использование условной взаимной информации между сообщениями при заданном M подчеркивает, что сообщения X^{in} и X^{out} принадлежат одному и тому же сеансу связи, а именно тому, в котором передается информационное сообщение M. Совершенная несвязываемость гарантирует, что наблюдая сообщения, принадлежащие одному сеансу связи, в разных точках маршрута, нельзя установить, что эти сообщения действительно принадлежат одному сеансу связи.

Пусть подслушав сообщение X^{in}, злоумышленник получил W^{in}, то есть $W^{in}=g(X^{in})$, $g:\mathbb{X}\to\mathbb{W}$, а подслушав X^{out}, он получил W^{out}. Тогда

Определение 1.10. *Сообщения X^{in} и X^{out} называются совершенно несвязываемыми с точки зрения злоумышленника, если $I(W^{in}; W^{out}|M) = 0$.*

Использование условной взаимной информации подчеркивает, что информация полученная злоумышленником, то есть сообщения W^{in}, W^{out} относятся к одному и тому же сеансу связи. В общем случае информационное сообщение M может быть как известно злоумышленнику, так и неизвестно. Далее будет показано, что для методов, предлагаемых в диссертационной работе, необходимо, чтобы сообщение M не было известно злоумышленнику.

1.7 Выводы

В этой главе:

1) даны основные определения анонимной передачи данных;

2) описаны модели злоумышленников;

3) представлен сравнительный анализ методов анонимности для традиционных сетей и для сетевого кодирования;

4) представлен сравнительный анализ численных характеристик оценки анонимности;

5) предложено понятие совершенной несвязываемости сообщений.

Глава 2

Анонимность для цифрового сетевого кодирования и традиционной маршрутизации

В этой главе диссертационной работы будет предложен теоретико-информационный метод обеспечения несвязываемости для когерентного сетевого кодирования. Будет рассмотрен случай пассивного [14, 15] (раздел 2.4) и активного злоумышленников [16] (раздел 2.5). Также в этой главе диссертационной работы будет описан теоретико-информационный метод обеспечения несвязываемости сообщений для традиционной маршрутизации (раздел 2.6).

Прежде чем излагать суть предлагаемого метода приведем все сведения необходимые для его описания. В разделе 2.1 введем основные понятия из алгебры и теории кодирования, в разделе 2.2 будет изложен принцип сетевого кодирования и даны необходимые понятия из теории ранговых кодов, которые используются в сетевом кодировании, а в разделе 2.3 будут изложены известные результаты из теории канала с подслушиванием, на основе которого строится предлагаемый метод.

2.1 Основные понятия

Пусть $G = (S, +)$ – группа, а $H = (T, +)$, $T \subset S$ – подгруппа группы G.

Определение 2.1. *Пусть $a \in G$. Множество $a + H$ называется левосторонним смежным классом группы G по подгруппе H. Множество $H + a$ называется правосторонним смежным классом группы G по подгруппе H.*

Утверждение 2.1 ([59])**.** *Всякий смежный класс определяется любым своим элементом.*

Утверждение 2.2 ([59]). *Смежные классы либо не пересекаются, либо совпадают. Это значит, что при заданной подгруппе $H \subset G$ каждый элемент $a \in G$ принадлежит в точности одному смежному классу.*

Вся группа G распадается на непересекающиеся смежные классы по подгруппе H.

$$G = (a_0 + H) \cup (a_1 + H) \cup (a_2 + H) \cup \ldots \cup (a_j + H) \cup \ldots,$$

Утверждение 2.3 ([59]). *Все смежные классы равномощны.*

Пусть $\mathbb{F}_q$ – конечное поле, состоящее из q элементов, q – степень простого числа. Пусть $\mathbb{F}_{q^m}$ – расширение поля $\mathbb{F}_q$ степени m, где m – натуральное число. Поле $\mathbb{F}_q$ называется базовым полем, поле $\mathbb{F}_{q^m}$ называется расширенным полем. Пусть X^n – n-мерное векторное пространство над полем $\mathbb{F}_{q^m}$.

Определение 2.2. *Линейным кодом C длины n и размерности k над полем $\mathbb{F}_{q^m}$ называется k-мерное линейное подпространство пространства X^n.*

Определение 2.3. *Пусть на X^n задана некоторая метрика $d(x, y)$, $x, y \in X^n$. Минимальным расстоянием или просто расстоянием кода C называется величина*

$$d(C) = d = \min\{d(x, y) | x \in C, y \in C, x \neq y\}.$$

Определение 2.4. *Пусть $x = (x_1, x_2, \ldots, x_n) \in X^n$. Весом $w(x)$ вектора x называется число отличных от нуля его компонент.*

Если код имеет расстояние d, то он может исправлять все ошибки веса $w(e) \leq t = \lfloor \frac{d-1}{2} \rfloor$. Величина t называется *корректирующей способностью* кода.

Линейный код длины n, размерности k с расстоянием d называют (n, k, d)-кодом.

Теорема 2.1 (Граница Синглтона, [59]). *Для любого (n, k, d) кода верно неравенство*

$$d \leq n - k + 1.$$

Пусть $g_1 = (g_{11}, \ldots, g_{1n})^\top, g_2 = (g_{21}, \ldots, g_{2n})^\top, \ldots, g_k = (g_{k1}, \ldots, g_{kn})^\top$ есть k линейно независимых векторов пространства X^n.

Определение 2.5. *Матрица*

$$\mathbf{G} = (g_{ij}),\ i = 1, 2, \ldots, k,\ j = 1, 2, \ldots, n,$$

называется порождающей матрицей (n, k) кода.

Пусть $m = (m_1, \ldots, m_k)^\top$ – информационный вектор. Соответствующий кодовый вектор задаётся в виде $x = \mathbf{G}^\top m$.

Для любой матрицы $\mathbf{G}$ ранга k существует $(n-k) \times k$ матрица $\mathbf{H}$ полного ранга $n-k$ такая, что $\mathbf{G}\mathbf{H}^\top = 0$.

Определение 2.6. *Матрица* $\mathbf{H}$ *называется проверочной матрицей кода.*

Пусть $x \in C$ и $y = x + e$ $y \in X^n$. Тогда $\mathbf{H}y = \mathbf{H}x + \mathbf{H}e = \mathbf{H}e$, так как $\mathbf{H}x = 0$.

Определение 2.7. *Величина* $\mathbf{H}e = s$ *называется синдромом.*

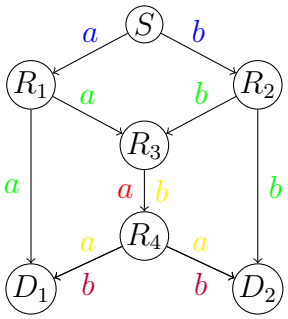
Пусть $X^n = C_0 \cup C_1 \cup C_2 \cup \ldots \cup C_{q^{m(n-k)}-1}$ есть разложение пространства X^n по подпространству $C = C_0$ и C_i, $i = 1, 2, \ldots, q^{m(n-k)} - 1$ суть смежные классы.

Теорема 2.2 ([59])**.** *Все векторы одного и того же смежного класса имеют одинаковые синдромы. Различным смежным классам отвечают различные синдромы.*

2.2 Цифровое сетевое кодирование

В настоящее время передача данных во всех сетях осуществляется посредством маршрутизации. Во время маршрутизации промежуточные узлы принимают входящие пакеты данных и без изменения передают их дальше. Можно сказать, что промежуточные узлы выполняют тождественное преобразование. *Сетевое кодирование* обобщает идею маршрутизации, позволяя промежуточным узлам выполнять любое преобразование над поступившими пакетами, что может приводить к увеличению пропускной способности сети. С момента своего появления сетевое кодирование активно исследуется. Появляются как теоретические результаты, так и практически применимые решения. Наиболее изучено линейное сетевое кодирование, идея которого состоит в том, что промежуточные узлы передают дальше линейные комбинации принятых пакетов.

По способу интеграции с TCP/IP стеком сетевое кодирование можно условно разделить на аналоговое и цифровое. Под аналоговым будем понимать сетевое кодирование, которое используется на физическом уровне, то есть применяется непосредственно к передаваемым сигналам. Все уровни стека TCP/IP выше физического оперируют с битовыми данными, поэтому сетевое кодирование, применяемое на этих уровнях, будем называть цифровым. Идея сетевого кодирования была предложена в работе [12]. Сетевое кодирование определялось как процесс кодирования, выполняемый узлами сети, где под кодированием понималось произвольное преобразование входных сообщений. Выполнение произвольных операций над поступившими сообщениями является главным отличием сетевого кодирования от традиционного способа передачи, где узлы сети просто передают дальше принятые сообщения без изменений.



(а) Традиционный способ передачи

(б) Сетевое кодирование

Рис. 2.1: Пример многоадресной передачи

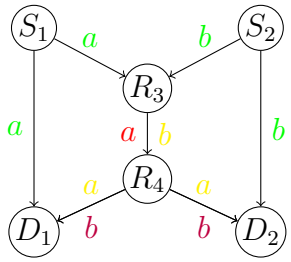
В настоящее время наиболее изученный сценарий передачи данных, где преимущество сетевого кодирования очевидно, – это многоадресная передача. Основное преимущество заключается в увеличении пропускной способности. Рассмотрим пример, впервые приведенный в работе [12] и известный под названием «бабочка». Источник S должен передать два сообщения a и b получателям D_1 и D_2. В работе [12] показано, что для достижения максимальной пропускной способности при многоадресной передаче некоторый промежуточный узел должен выполнить операцию сетевого кодирования. В качестве операции предлагается сумма по модулю два, в предположении, что сообщения a, b двоичные. При традиционном способе передачи для того, чтобы передать два сообщения a, b обоим получателям, необходимо пять сеансов передачи (рис. 2.1а). Различные цвета на рисунках обозначают различные сеансы передач. В случае сетевого кодирования промежуточный узел R_3 передаёт далее не два сообщения a и b по очереди, а одно сообщение – $a \oplus b$ (рис. 2.1б), что экономит один сеанс передачи. В итоге понадобится четыре сеанса передачи.

С помощью сетевого кодирования можно достичь увеличения пропускной способности и в случае нескольких одноадресных передач. На рисунке 2.2 представлен случай двух одноадресных передач.

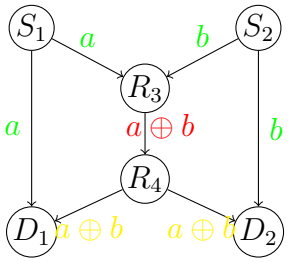
Эти два приведенных примера для случая многоадресной и одноадресной передачи являются наиболее простыми и яркими иллюстрациями идеи сетевого кодирования.

2.2.1 Основные сведения теории ранговых кодов

Приведем необходимые для понимания дальнейшего материала основные сведения теории ранговых кодов [60]. Пусть $\mathbb{X}^n - n$-мерное векторное пространство над полем $\mathbb{F}_{q^m}$, где $q-$степень простого числа. Будем рассматривать $\mathbb{F}_{q^m}$ как векторное пространство над $\mathbb{F}_q$ и зафиксируем базис $\Omega = \begin{pmatrix} \omega_1, & \omega_2, & \ldots, & \omega_m \end{pmatrix}$ поля $\mathbb{F}_{q^m}$. Тогда любой элемент $x_i \in \mathbb{F}_{q^m}$ можно единственным образом представить в виде $x_i = a_{1i}\omega_1 + a_{2i}\omega_2 + \ldots + a_{mi}\omega_m$. Следовательно, каждому вектору



(а) Традиционный способ передачи



(б) Сетевое кодирование

Рис. 2.2: Пример двух одноадресных передач

$x = \begin{pmatrix} x_1, & x_2, & \ldots, & x_n \end{pmatrix}$ можно поставить в соответствие единственную матрицу

$$\mathbf{A}(x) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \tag{2.1}$$

и определить ранг вектора x над $\mathbb{F}_q$, обозначается $r(x;q)$, как ранг матрицы $\mathbf{A}(x)$. Это определение имеет простой смысл: ранг вектора – это максимальное число его компонент, линейно независимых над $\mathbb{F}_q$. Аналогично можно определить ранг матрицы. Рангом матрицы $\mathbf{B}$ с элементами из $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$, обозначается $r(\mathbf{B};q)$, называется максимальное число линейно независимых над $\mathbb{F}_q$ столбцов. Определение ранга матрицы, известное из курса линейной алгебры, в настоящих обозначениях задаётся в виде $r(\mathbf{B};q^m)$. Это максимальное число столбцов или строк линейно независимых над $\mathbb{F}_{q^m}$. Столбцевой ранг матрицы B над $\mathbb{F}_{q^m}$ совпадает со строковым рангом над $\mathbb{F}_{q^m}$, что неверно для ранга над $\mathbb{F}_q$. Выполняется соотношение $r(\mathbf{B};q) \geq r(\mathbf{B};q^m)$.

Отображение $x \to r(x;q)$ есть норма на $\mathbb{X}^n$, так как удовлетворяет всем аксиомам нормы

1) $\forall x \in \mathbb{X}^n,\ r(x;q) \geq 0$ и $r(x;q) = 0 \Leftrightarrow x = 0$ (очевидно, что $1 \leq r(x;q) \leq \min(n,m)$),

2) $r(x+y;q) \leq r(x;q) + r(y;q)$ (так как ранг суммы матриц не превосходит суммы рангов),

3) если рассматривать элемент α из $\mathbb{F}_{q^m}$ как скаляр над $\mathbb{F}_{q^m}$, то $r(\alpha;q) = 1$, если $\alpha \neq 0$ и $r(\alpha;q) = 0$, если $\alpha = 0$, то $r(\alpha x;q) = r(\alpha;q)r(x;q)$.

Тогда можно определить *ранговую метрику.*

Определение 2.8. *Ранговое расстояние над полем $\mathbb{F}_q$ между векторами $x, y \in \mathbb{F}_{q^m}$ есть*

$$d(x,y) = r(x-y;q).$$

Минимальное ранговое расстояние $d(C) = d$ кода C определяется в виде

$$d = \min\{d(x, y) | x, y \in C, x \neq y\}.$$

Можно показать, что для кода с ранговым расстоянием d существует способ декодирования, при котором исправляются любые ошибки с рангом не более чем $\lfloor \frac{d-1}{2} \rfloor$.

Лемма 2.1 (Лемма 1 [60]). *Пусть на* $\mathbb{X}^n$ *заданы две нормы* r_1 *и* r_2, *причём* $r_1(x) \leq r_2(x)$, $\forall x$. *Пусть* $M_1(n, d)$ *и* $M_2(n, d)$ *– наибольшие мощности кодов с расстоянием* d *в соответствующих метриках. Тогда*

$$M_1(n, d) \leq M_2(n, d).$$

Выберем $r_1 = r(x; q)$, а в качестве r_2 возьмём вес Хэмминга $r_2 = r_H(x)$. Ясно, что $r(x; q) \leq r_H(x)$. Тогда согласно лемме 2.1 и известной границы Синглтона верно следующее утверждение.

Утверждение 2.4 ([60]). *Для* (n, k, d) *рангового кода при* $n \leq m$ *выполняется*

$$k \leq n - d + 1. \tag{2.2}$$

Определение 2.9. *Код* C, *достигающий границы 2.2, называется кодом с максимальным ранговым расстоянием (MPP).*

При $n \leq m$ (n, k) MPP код существует для любых допустимых значений n и k. Приведем конструкцию MPP кода. Обозначим $[i] = q^i$. Выберем n линейно независимых над $\mathbb{F}_q$ элементов поля $\mathbb{F}_{q^m}$. Обозначим их как $h_1, h_2, \ldots, h_n$. Образуем матрицу

$$\mathbf{H} = \begin{pmatrix} h_1 & h_2 & \ldots & h_n \\ h_1^{[1]} & h_2^{[1]} & \ldots & h_n^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \ldots & h_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \ldots & h_n^{[d-2]} \end{pmatrix}. \tag{2.3}$$

Теорема 2.3. *Код с проверочной матрицей (2.3) является MPP кодом длины* n *и с ранговым расстоянием* $d = n - k + 1$.

Теорема 2.4. *Пусть* $C-$*код с проверочной матрицей (2.3). Тогда порождающая матрица этого кода имеет вид*

$$\mathbf{G} = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_1^{[1]} & g_2^{[1]} & \ldots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \ldots & g_n^{[k-1]} \end{pmatrix}, \tag{2.4}$$

где $k = n - d + 1$, *а* $g_1, g_2, \ldots, g_n$ *линейно независимы над* $\mathbb{F}_q$.

Любой MPP код длины $n \leq m$ является также МДР кодом.

Для длин $n > m$ верна граница

$$km \leq (m - d + 1)n.$$

Для таких длин нельзя построить MPP код с помощью конструкции (2.4), так как набор $g_1, g_2, \ldots, g_n$ будет содержать элементы линейно зависимые над $\mathbb{F}_q$. Для длин $n > m$ можно строить *приведённые* ранговые коды [61]. Но в отличие от кодов Габидулина длины $n \leq m$, которые являются оптимальными как в ранговой так и в хэмминговой метрике, приведённые коды, оптимальные в ранговой метрике, могут иметь небольшое хэмминговое расстояние.

2.2.2 Теоретические основы сетевого кодирования

Рассмотрим основную задачу передачи данных в сетевом кодировании – многоадресную передачу с одним источником. Сеть задана направленным ациклическим мультиграфом $G = (V, E)$, где V – множество узлов сети, а E – множество соединений сети единичной пропускной способности, передача по котором происходит без ошибок. Источник $S \in V$ генерирует r битовых информационных потоков $X_1, X_2, \ldots, X_r$. Все потоки источника должны быть переданы каждому элементу множества получателей $T \subset V \backslash S$. Решением этой задачи являются кодовые операции на промежуточных узлах и операция декодирования на узлах-получателях, такая что каждый получатель восстанавливает все информационные потоки источника. Каждый получатель $t \in T$ формирует полученные им потоки $Z_{t,1}, Z_{t,2}, \ldots, Z_{t,r}$ как сумму входных потоков. Задача решена, если $Z_{t,i} = X_i,\ \forall t \in T,\ i = 1, 2, \ldots, r$.

Поток $X_i,\ i = 1, 2, \ldots, r$ разбивается на группы по m бит, и каждая такая группа рассматривается как элемент поля $\mathbb{F}_q,\ q = 2^m$. Тогда поток $X_i,\ i = 1, 2, \ldots, r$ можно рассматривать как вектор над полем $\mathbb{F}_q$. Пусть для ребра l $o(l)$ обозначает начальную вершину ребра, а $d(l)$ – конечную вершину ребра. $I(v), O(v)$ обозначают соответственно множества входных и выходных рёбер вершины v. Каждый j-й символ, передаваемый по ребру l есть линейная в $\mathbb{F}_q$ функция j-х символов всех потоков, входящих в узел $o(l)$. Так как эта функция одинакова для всех значений j, то для того, чтобы рассмотреть передачу некоторого потока, достаточно рассмотреть передачу одного его символа. Через x_i обозначим символ i-го потока, а через y_l символ, передаваемый по ребру l. Тогда для ребра l можно записать

$$y_l = \sum_{k \in I(o(l))} f_{k,l} y_k + \begin{cases} \sum_{i=1}^{r} a_{i,l} x_i, \text{ если } o(l) = S, \\ 0, \text{ иначе,} \end{cases} \tag{2.5}$$

где $f_{k,l}, a_{i,l}$ – элементы $\mathbb{F}_q$, называемые *локальными кодирующими коэффициентами*. Векторы $\mathbf{a} = (a_{i,l},\ 1 \leq i \leq r,\ l \in E),\ \mathbf{f} = (f_{k,k},\ k, l \in E)$ называются *локальными кодирующими*

векторами. Так как все операции линейны, то

$$y_l = \sum_{i=1}^{r} c_{i,l} x_i,$$

где $c_{i,l}$ называются *глобальными кодирующими коэффициентами*. Каждый получатель имеет

$$z_{t,i} = \sum_{k \in I(t)} b_{t,i,k} y_k, \tag{2.6}$$

где $b_{t,i,k}$ можно считать коэффициентами декодирования, а вектор $\mathbf{b} = (b_{t,i,k},\ t \in T,\ 1 \leq i \leq r,\ k \in E)$ вектором декодирования. Перепишем уравнение (2.5) в матричной форме

$$\mathbf{y} = \mathbf{y}\mathbf{F} + \mathbf{x}\mathbf{A},$$

где $\mathbf{F} = (f_{k,l}) \in \mathbb{F}_q^{|E| \times |E|}$, $f_{k,l} = 0$, если $d(k) \neq o(l)$, $\mathbf{A} = (a_{i,l}) \in \mathbb{F}_q^{r \times |E|}$. Ребра графа G можно топологически отсортировать так, что если для $e_i, e_j \in E$ выполняется $o(e_i) = d(e_j)$, то $j < i$. Тогда матрица $\mathbf{F}$ будет верхней диагональной с нулями по диагонали и, следовательно, матрица $\mathbf{I} - \mathbf{F}$, где $\mathbf{I}$ – единичная матрица, будет невырожденной.

$$\mathbf{y} = \mathbf{x}\mathbf{A}(\mathbf{I} - \mathbf{F})^{-1}.$$

Матрицу $\mathbf{C} = \mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}$ называют *кодирующей* или *матрицей передачи*. Перепишем уравнение (2.6) в матричной форме

$$\mathbf{z}_t = \mathbf{y}\mathbf{B}_t^{\top}.$$

Тогда

$$\mathbf{z}_t = \mathbf{x}\mathbf{A}(\mathbf{I} - \mathbf{F})^{-1}\mathbf{B}_t^{\top}.$$

Решением этой задачи многоадресной передачи в сетевом кодировании являются матрицы $\mathbf{A}, \mathbf{F}, \mathbf{B}_t$ такие, что $\mathbf{A}(\mathbf{I} - \mathbf{F})^{-1}\mathbf{B}_t^{\top} = \mathbf{I}\ \forall t \in T$.

Существование решения опирается на теорему Форда-Фалкерсона для одноадресной передачи.

Теорема 2.5 (Форда-Фалкерсона)**.** *Следующие утверждения эквивалентны.*

1. *Между источником s и получателем t существует поток скорости r.*

2. *Величина минимального разреза между s и t не менее r.*

Одноадресную передачу можно рассматривать как вырожденный случай многоадресной передачи: источник s передаёт r информационных потоков множеству получателей T, $|T| = 1$. В этом свете к двум утверждениям теоремы Форда-Фалкерсона можно добавить ещё одно, выраженное в терминах сетевого кодирования, а именно

3. *Матрица* $\mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}\mathbf{B}_t^\top$ *невырождена в кольце полиномов* $\mathbb{F}_2[\mathbf{a},\mathbf{f},\mathbf{b}]$.

Теорема 2.6 (Теорема 2.1 [62]). *Условия 1 и 3 эквивалентны.*

Теорема 2.7 (Теорема 2.2 [62]). *Задача многоадресной передачи в сетевом кодировании разрешима тогда и только тогда, когда существует поток скорости r между источником s и каждым получателем $t \in T$.*

Смысл теоремы 2.7 состоит в том, что если передача информации со скоростью r возможна между источником и каждым получателем, то с помощью сетевого кодирования возможно передавать информацию со скоростью r всем получателям одновременно.

Если задача разрешима, то известно два способа построить сетевой код. По способу построения сетевого кода линейное сетевое кодирование разделяется на *когерентное* и *некогерентное*. В случае когерентного сетевого кодирования код строится централизованно с учетом топологии сети. В [62] приведен алгоритм построения кода со сложностью $O(|A|(r+|T|)|T|r)$, а также показано, что алфавита размера $q \geq |T|$ достаточно для решения задачи, иными словами задача многоадресной передачи в сетевом кодировании может быть решена в поле $\mathbb{F}_{|T|}$.

В работе [63] было предложено выбирать кодирующие векторы $\mathbf{a},\mathbf{f}$ случайно из достаточно большого поля. Этот способ построения получил название некогерентного или случайного сетевого кодирования. Случайно выбранные кодирующие векторы будут решением задачи с некоторой вероятностью. Этот вид сетевого кодирования в диссертационной работе не рассматривается.

На практике информация передается пакетами. Сообщения источников состоят из некоторого количества пакетов, а пакеты в свою очередь состоят из некоторого количества бит. Рассматривая m последовательных бит как элемент поля $\mathbb{F}_q$, $q=2^m$, пакеты можно рассматривать как векторы над полем $\mathbb{F}_q$, а сообщения как матрицы, строками которой являются пакеты. При передаче по сети промежуточные узлы формируют линейные комбинации строк информационных матриц. Такой канал связи описывается соотношением

$$\mathbf{Y} = \mathbf{A}\mathbf{X},$$

где $\mathbf{X} \in \mathbb{F}_q^{n\times N}$ – информационная матрица источника, состоящая из n пакетов длины N, $\mathbf{A}$ – матрица передачи, то есть матрица, имеющая смысл матрицы $\mathbf{C}$ в предыдущих обозначениях, а $\mathbf{Y} \in \mathbb{F}_q^{n_r\times N}$ – матрица пакетов, принятых получателем. В процессе передачи информационные матрицы могут подвергаться искажениям, связанными с возникающими в сети ошибками. В этом случае канал связи описывается соотношением

$$\mathbf{Y} = \mathbf{A}\mathbf{X} + \mathbf{B}\mathbf{Z},$$

где $\mathbf{Z}$ – это матрица, характеризующая ошибки, её строки представляют собой ошибочные пакеты, а $\mathbf{B}$ – матрица передачи ошибочных пакетов. Для борьбы с ошибками необходимо использовать некий метод кодирования источника. Удобно использовать ранговый код. В этом случае матрица $\mathbf{X}$ есть матричное представление кодового слова рангового кода (2.1). Линейные преобразования передаваемой информации во время её передачи по сети не меняют подпространства, заданного строками матрицы $\mathbf{X}$. Следовательно, информацию источника можно кодировать не в конкретную матрицу, а в подпространство. Так появилась идея подпространственных кодов [64, 65], тесно связанных с ранговыми кодами.

2.3 Канал с подслушиванием типа II

В работе [2] рассматривалась секретная передача сообщения по каналу с отводом. Этот канал называют каналом с подслушиванием типа II. Канал с отводом можно представить как два дискретных канала без памяти: основной и отводный. Основной – это канал между источником и получателем, передача по которому происходит без ошибок, а отводный – канал между источником и злоумышленником, который является каналом со стираниями.

Предположим, источник хочет передать по каналу сообщение S, состоящее из k символов. Сообщение должно быть передано секретно при наличии злоумышленника, способного прослушивать любое подмножество J передаваемых символов мощности не более чем заданная $|J| = \mu$. Секретность должна быть достигнута таким образом, чтобы отправителю и получателю сообщения не требовалось обладать каким-либо общим секретом.

Сообщение S рассматривается как случайная величина, заданная на множестве $\{0,1\}^k$. Пусть W – вектор длины n, который определяет информацию, поступающую к злоумышленнику. Тогда, μ элементов этого вектора точно известны – это μ символов сообщения, подслушанных злоумышленником, в остальных символах W произошли стирания. Через Δ обозначим следующую величину $\Delta = \min\limits_{J:\,|J|=\mu} H(S|W)$. Можно сказать, что Δ определяет количество символов сообщения S, которые остаются неизвестны злоумышленнику после того, как он получил W. Если возможно предложить метод кодирования сообщения S в сообщение $X \in \{0,1\}^n$ такой, что при передаче сообщения X значение Δ будет максимальным и равным k, то система является совершенно секретной. В этом случае злоумышленник не получает никакой информации о сообщении S источника. В работе [2] показано, что $\forall \epsilon > 0, n_0 \geq 1$ существует $n \geq n_0$, кодер $f_E : \{0,1\}^k \to \{0,1\}^n$ и декодер $f_D : \{0,1\}^n \to \{0,1\}^k$ с параметрами $k = Rn,\ \mu = \alpha n,\ \frac{\Delta}{k} \geq ((\frac{1-\alpha}{R})) - \epsilon$ и вероятности ошибки $P_e = 0$, где R и α – параметры, связанные соотношением $1 - R \leq \alpha \leq 1$.

Это метод кодирования может быть реализован с помощью группового кода. Разбиваем множество $\{0,1\}^n$ на 2^k подмножеств $\{A_m\}_{m=1}^{2^k}$ одинаковой мощности $|A_m| = 2^{n-k}$. Пусть $\mathbf{H}$ – про-

верочная матрица размера $k \times n$ и ранга k. Разбиение $\{A_m\}$ определяет код, заданный $\mathbf{H}$, и его смежные классы. Можно установить взаимно однозначное соответствие между значениями S и разбиением $\{A_m\}$. Чтобы закодировать сообщение $S \in \{0,1\}^k$ кодер произвольным образом выбирает X как один из 2^{n-k} элементов смежного класса, определяемого синдромом S. Это эквивалентно тому, что X есть произвольно выбранное решение из 2^{n-k} решений уравнения $\mathbf{H}X = S$. Так как множества $\{A_m\}$ не пересекаются, декодер может восстановить S без ошибок простым вычислением синдрома $S = \mathbf{H}X$. При этом

$$\Delta = \begin{cases} n-\mu,\ n-d+1 \le \mu \le n, \\ k,\ 0 \le \mu \le d'-1, \end{cases} \tag{2.7}$$

где d – расстояние кода, d' – расстояние двойственного кода. Если код с проверочной матрицей $\mathbf{H}$ есть код с максимальным расстоянием (МДР), то двойственный код также есть МДР код, то есть $d'-1 = n-k$, и тогда можно передать k бит секретно при $\mu \le n-k$.

Если n символов сообщения X передаются по сети, то k из них также могут быть переданы секретно по методу кодирования смежными классами, если злоумышленник прослушивает не более чем μ соединений. В работе [8] показано, что это необязательно выполняется, если сеть работает по принципу сетевого кодирования. В этой работе рассматривается случай когерентного сетевого кодирования, а метод кодирования смежными классами строится на основе $(n, n-k)$ МДР кода на полем $\mathbb{F}_q$, где q достаточно большое. Пусть $\mathbf{H}$ – $k \times n$ проверочная матрица $(n, n-k)$ МДР кода, а $\mathbf{C}$ – кодирующая матрица сетевого кода, её строками являются кодирующие векторы соединений сети. Тогда через $\mathbf{C}_J$ можно обозначить матрицу, строки которой есть кодирующие векторы соединений сети, прослушиваемых злоумышленником. Её размер равен $\mu \times n$. Злоумышленник может выбирать соединения так, что $\mathrm{Rk}(\mathbf{C}_J) = \mu$. Если источник хочет секретно передать сообщение $S \in \mathbb{F}_q^k$, то он передает сообщение $X \in \mathbb{F}_q^n$, где S и X связаны соотношением $S = \mathbf{H}X$. Злоумышленник может подслушать $W \in \mathbb{F}_q^\mu$, где $W = \mathbf{C}_J X$. Для того чтобы S было передано секретно, S и W должны быть статистически независимы, т.е. должно выполняться $H(S|W) = H(S)$.

$$H(SXW) = H(W) + H(S|W) + H(X|SW) = H(W) + H(X|W) + H(S|XW)$$
$$\underset{=H(S)}{H(S|W)} + H(X|SW) = H(X|W) + \underset{=0}{H(S|XW)}$$
$$H(X|SW) = H(X|W) - H(S)$$

Так как $H(X|W) \le \log_q |\mathbb{X}_w|$, где $\mathbb{X}_w = \{x \in \mathbb{F}_q^n | w = \mathbf{C}_J x\}$ и $|\mathbb{X}_w| = q^{n-\mathrm{Rk}\mathbf{C}_J}$, то

$$H(X|W) \le n - \mathrm{Rk}(\mathbf{C}_J) = n - \mu.$$

Тогда

$$0 \le H(X|SW) \le n - \mu - k.$$

При $\mu = n - k$ выполняется $H(X|SW) = 0$ и система

$$\begin{pmatrix} S \\ W \end{pmatrix} = \begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix} X$$

имеет единственное решение для любого J, такого что $\mathrm{Rk}(\mathbf{C}_J) = \mu$. Тогда

$$\mathrm{Rk} \begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix} = n.$$

Последнее равенство дает критерий построения сетевого кода – строковое пространство матрицы $\mathbf{C}_J$ не должно пересекаться со строковым пространством матрицы $\mathbf{H}$.

Авторы статьи [9] Силва и Кшишанг разделили метод кодирования смежными классами и сетевой код. Они доказали, что если $\mathbf{H}$ – это проверочная матрица кода с максимальным ранговым расстоянием (MPP) [60], то условие

$$\mathrm{Rk} \begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix} = \mathrm{Rk}(\mathbf{H}) + \mathrm{Rk}(\mathbf{C}_J)$$

выполнено для любой матрицы $\mathbf{C}_J \in \mathbb{F}_q^{\mu \times n}$. Ранговая метрика играет ключевую роль в доказательстве этого утверждения. Доказательство основано на том, что если ранг ненулевого вектора $x \in \mathbb{F}_{q^m}^n$ не превосходит k, то существует матрица $\mathbf{B} \in \mathbb{F}_q^{(n-k)\times n}$ ранга $n - k$ такая, что $\mathbf{B}x = 0$. И обратно, если $\mathbf{B}x = 0$ для ненулевого $x \in \mathbb{F}_{q^m}^n$ и матрицы полного ранга $\mathbf{B} \in \mathbb{F}_q^{(n-k)\times n}$, то ранг вектора x не превосходит k. Действительно, если ранг вектора x не превосходит k, то этот вектор можно представить в виде $x = \mathbf{D}z$, где $z \in \mathbb{F}_{q^m}^k$, а $\mathbf{D} - n \times k$ матрица над $\mathbb{F}_q$ ранга k. Для $\mathbf{D}$ существует ортогональная ей матрица $\mathbf{Q} \in \mathbb{F}_q^{n\times(n-k)}$ ранга $n - k$. Тогда $\mathbf{Q}^\top \mathbf{D}z = 0$. Полагая $\mathbf{B} = \mathbf{Q}^\top$, получим первую часть вышеописанного утверждения. Если $\mathbf{B}x = 0$ при условии, что ранг $\mathbf{B}$ равен $n - k$, то x принадлежит пространству ортогональному строковому пространству матрицы $\mathbf{B}$, то есть $\underbrace{\mathbf{B}\mathbf{Q}^\top}_{=0} z = 0,\ \mathbf{Q} \in \mathbb{F}_q^{k\times n},\ \mathrm{Rk}\mathbf{Q} = k,\ z \in \mathbb{F}_{q^m}^k$. Следовательно, x представим в виде $x = \mathbf{Q}^\top z$, что в свою очередь означает, что ранг x не более k. Теперь матрицу $\begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix}$ можно преобразовать в матрицу $\mathbf{L} = \begin{pmatrix} \mathbf{H} \\ \mathbf{B} \end{pmatrix}$ размера $n \times n$ с помощью двух матриц полного ранга $\mathbf{T}$ и $\mathbf{D}$ как $\mathbf{B} = \begin{pmatrix} \mathbf{T}\mathbf{C}_J \\ \mathbf{D} \end{pmatrix} \in \mathbb{F}_q^{(n-k)\times n}$. Причем выполняется $\mathrm{Rk}\mathbf{L} \leq \mathrm{Rk} \begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix}$. Если $\mathrm{Rk} \begin{pmatrix} \mathbf{H} \\ \mathbf{C}_J \end{pmatrix} < \mathrm{Rk}\mathbf{H} + \mathrm{Rk}\mathbf{C}_J$, то $\mathrm{Rk}\mathbf{L} < n$. Но если $\mathrm{Rk}\mathbf{L} < n$, то существует ненулевой вектор $x \in \mathbb{F}_{q^m}^n$ такой, что $\mathbf{L}x = 0$. Из этого следует, что $\mathbf{H}x = 0$, то есть x принадлежит MPP коду, заданному проверочной матрицей $\mathbf{H}$. Тогда ранг x не менее рангового расстояния кода, то есть не менее $k + 1$. С другой стороны из $\mathbf{L}x = 0$ также следует, что $\mathbf{B}x = 0$. Последнее приводит к тому,

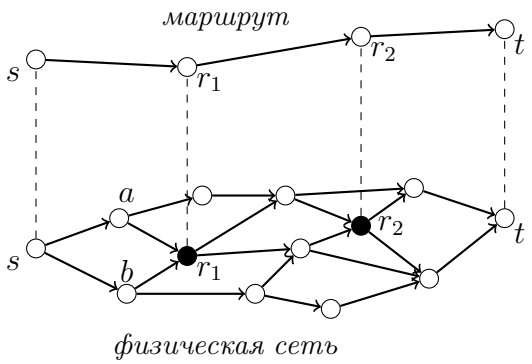


Рис. 2.3: Формирование маршрута

что ранг вектора x не превосходит k. Полученное противоречие свидетельствует о неверности первоначального предположения о том, что

$$\mathrm{Rk}\begin{pmatrix}\mathbf{H}\\ \mathbf{C}_J\end{pmatrix} < \mathrm{Rk}\mathbf{H} + \mathrm{Rk}\mathbf{C}_J.$$

2.4 Пассивный злоумышленник

2.4.1 Модель сети

Сеть представлена направленным мультиграфом $G(V, E)$, вершины V которого есть узлы сети, а ребра E –линии связи с единичной пропускной способностью. Это значит, что в единицу времени по каждому соединению передаётся один пакет данных. Сообщения передаются по принципу когерентного сетевого кодирования без ошибок. В сети присутствуют N источников сообщений и N получателей, между которыми осуществляется одноадресная передача.

Предполагается, что между источниками и получателями установлены маршруты. Маршрут представляет собой упорядоченный набор узлов сети, которые могут восстановить сообщение предыдущего узла (рис. 2.3). Это означает, что количество реберно непересекающихся путей между любыми двумя последовательными узлами маршрута равно количеству пакетов, образующих сообщение. Если по сети передаются сообщения, состоящие из n пакетов, то таких путей должно быть не менее n. Таким образом, источник, получатель и маршрут между ними формируют оверлейную сеть. На рисунке 1.4 представлен случай для $n = 2$, где существует два реберно непересекающихся пути между источником $S_i,\ i = 1, 2$ и узлом r, а также два реберно непересекающихся пути между узлом r получателем D_i, а именно $r \to D_1,\ r \to u \to D_1$ для $i = 1$ и $r \to D_2,\ r \to v \to D_2$ для $i = 2$. Пусть передаётся сообщение X состоящее из n пакетов. По каждому соединению передаётся линейная комбинация пакетов, то есть $c_i X,\ i = 1, 2 \ldots$, где c_i – кодирующий вектор ребра. Каждый промежуточный узел получает сообщение вида $\mathbf{A}X$,

где $\mathbf{A} \in \mathbb{F}_q^{n \times n}$ – матрица передачи. Кодирующие векторы задаются над полем $\mathbb{F}_q$. Матрица $\mathbf{A}$ имеет размер $n \times n$ и ранг n. Этим обеспечивается возможность восстановления сообщения X каждым промежуточным узлом. Узел r_1 (рис. 2.3) получит сообщение $\mathbf{A}_{r_1}X$, где $\mathbf{A}_{r_1}$ – матрица передачи от источника s до r_1, узел r_2 получит $\mathbf{A}_{r_2}X$, где $\mathbf{A}_{r_2}$ – матрица передачи от источника до r_2, причём $\mathbf{A}_{r_2} = \mathbf{A}_{r_1-r_2}\mathbf{A}_{r_1}$, где $\mathbf{A}_{r_1-r_2}$ – матрица передачи между r_1 и r_2.

Предполагается, что маршрут может быть сформирован таким образом, что узлы, не участвующие в передаче, не обладают о нём никакой информацией. Промежуточные узлы маршрута обладают информацией только о своих ближайших соседях, то есть им известно кому дальше передать пакеты, принятые от конкретного предыдущего узла. В когерентном сетевом кодировании задача маршрутизации связана с задачей построения сетевого кода. А именно, построение сетевого кода отчасти аналогично задаче статической маршрутизации. Для обеспечения анонимности сетевой код должен быть построен таким образом, чтобы он не раскрывал маршрутной информации. Например, проанализировав матрицы передачи между всеми возможными парами источник-получатель, злоумышленник может определить, что некоторые из этих пар узлов не могут обмениваться сообщениями, так как матрица передачи между ними не имеет полного ранга. На рисунке 1.4 матрица передачи от S_1 к D_1 равна $\begin{pmatrix} 4 & 6 \\ 5 & 7 \end{pmatrix}$. Её ранг равен 2. Ранг матрицы передачи $\begin{pmatrix} 2 & 3 \\ 6 & 9 \end{pmatrix}$ от S_1 к D_2 равен 2. Ранги матриц передач от S_2 к D_2 и от S_2 к D_2 также равны 2. Таким образом, анализ матриц передачи не позволяет злоумышленнику выделить возможные пары источник-получатель.

2.4.2 Модель злоумышленника

Рассматриваются два типа злоумышленника: внешний пассивный адаптивный глобальный злоумышленник и внешний пассивный адаптивный локальный злоумышленник. Локальность второго злоумышленника заключается в том, что он не может прослушивать все входящие соединения и все выходящие соединения конкретного узла, а только не более чем μ входящих и не более чем μ выходящих. Среди всех прослушанных злоумышленником соединений должно быть не более μ входных соединений и не более μ выходных соединений, принадлежащих одному и тому же узлу. Так как по разным соединениям передаются разные линейные комбинации пакетов исходного сообщения, то злоумышленник может получить $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in}$ и $\mathcal{W}^{out} = \mathbf{B}^{out}\mathcal{X}^{out}$, где $\mathcal{X}^{in}$, $\mathcal{X}^{out}$ – входное и выходное сообщения узла соответственно, а $\mathbf{B}^{in}$, $\mathbf{B}^{out} \in \mathbb{F}_q^{\mu \times n}$ – матрицы кодирующих векторов входных и выходных соединений, прослушиваемых злоумышленником. Используемый источниками код C злоумышленнику известен.

Хотя в области защиты информации методы защиты разрабатываются всегда для худшего случая, то есть для самого сильного злоумышленника, который должен быть глобальным,

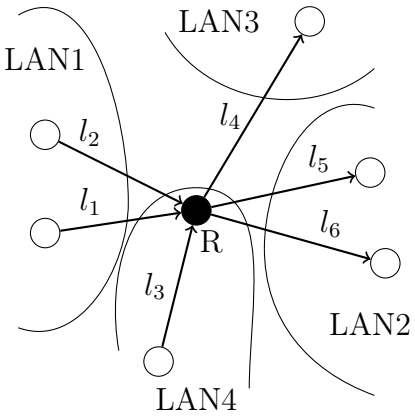


Рис. 2.4: Пример структуры сети

рассмотрение локального злоумышленника не лишено практического смысла. Ввиду географической распределённости и административного деления сетей злоумышленник не всегда имеет доступ ко всей передаваемой информации. Рассмотрим пример (рис. 2.4). Пусть узел R является одним из звеньев маршрута сообщения, отправителя и получателя которого пытается вычислить злоумышленник. Злоумышленник хочет прослушать пакеты, поступающие в узел R и отправляемые им. Узел R находится в локальной сети LAN4, к которой злоумышленник не имеет доступа, равно как и к сети LAN3. Но он имеет доступ к локальной сети LAN1 и LAN2, то есть может прослушать соединения $l_1,\ l_2,\ l_5,\ l_6$. Такого злоумышленника можно смоделировать как двух взаимодействующих злоумышленников, один из которых находится в сети LAN1, а другой в LAN2.

2.4.3 Кодирование источника

Источники передают в сеть пакеты. Соединения сети имеют единичную пропускную способность, то есть могут передавать один пакет. Пакет – это вектор длины m, координаты которого интерпретируются как элементы базового конечного поля $\mathbb{F}_q$. В одном сеансе каждый источник передаёт n пакетов, $n \leq m$. Другими словами, в сеансе передаётся матрица $\mathbf{X}$ размера $n \times m$ с элементами из поля $\mathbb{F}_q$, строками которой являются пакеты. Для формирования матрицы $\mathbf{X}$ источник использует кодирование. Фактически источник должен передать получателю $k < n$ равномерно распределённых информационных пакетов, которые можно представить в виде информационной матрицы $\mathbf{S}$ размера $k \times m$ над полем $\mathbb{F}_q$. Эта матрица преобразуется в кодовую матрицу $\mathbf{X}$. Получатель декодирует принятую матрицу $\mathbf{X}$, чтобы извлечь информационные пакеты $\mathbf{S}$.

Для кодирования источник использует коды MPP. Кодирование удобнее описывать в терминах операций в расширенном поле $\mathbb{F}_{q^m}$. Используя некоторый базис $\mathbf{\Omega} = \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_m \end{pmatrix}$ этого

поля над базовым полем $\mathbb{F}_q$, преобразуем матрицы $\mathbf{X}$ и $\mathbf{S}$ в векторы-столбцы $\mathcal{X} = \mathbf{X}\boldsymbol{\Omega}^\top \in \mathbb{F}_{q^m}^n$ и $\mathcal{S} = \mathbf{S}\boldsymbol{\Omega}^\top \in \mathbb{F}_{q^m}^k$.

Обозначим через $C\ (n, n-k)$ код с максимальным ранговым расстоянием $d = k+1$ над полем $\mathbb{F}_{q^m}$ с порождающей матрицей $\mathbf{G} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ и проверочной матрицей $\mathbf{H} \in \mathbb{F}_{q^m}^{k\times n}$.

Источники предварительно кодируют сообщения по схеме секретной передачи Силвы-Кшишанга [9]. Предположим, источник хочет секретно передать информационное сообщение $\mathcal{S} \in \mathbb{F}_{q^m}^k$. Источник строит сначала невырожденную матрицу $\mathbf{T}$ порядка n следующим образом:

$$\mathbf{T}^{-1} = \begin{pmatrix} \mathbf{H} \\ \mathbf{L} \end{pmatrix}.$$

где $\mathbf{L} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ – произвольная матрица, строки которой не являются линейными комбинациями строк матрицы $\mathbf{H}$. Обратная к ней матрица $\mathbf{T}$ записана в виде

$$\mathbf{T} = \begin{pmatrix} \mathbf{P}^\top & \mathbf{G}^\top \end{pmatrix}.$$

где $\mathbf{P} \in \mathbb{F}_{q^m}^{k\times n}$. Так как

$$\mathbf{T}^{-1}\mathbf{T} = \begin{pmatrix} \mathbf{I}_k & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{pmatrix},$$

то $\mathbf{H}\mathbf{P}^\top = \mathbf{I}_k$, а матрицы $\mathbf{L}$ и $\mathbf{P}$ связаны соотношением $\mathbf{L}\mathbf{P}^\top = \mathbf{0}$. Затем источник преобразовывает информационное сообщение $\mathcal{S}$ в кодовое сообщение $\mathcal{X} \in \mathbb{F}_{q^m}^n$ следующим образом:

$$\mathcal{X} = \mathbf{T}\begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix}, \tag{2.8}$$

где $\mathcal{V} \in \mathbb{F}_{q^m}^{(n-k)}$ – случайный независимый от $\mathcal{S}$ вектор с равномерным распределением. Из соотношения (2.8) следует, что вектор-столбец $\mathcal{X}$ можно представить как сумму двух векторов

$$\mathcal{X} = \mathbf{P}^\top\mathcal{S} + \mathbf{G}^\top\mathcal{V}. \tag{2.9}$$

При этом вектор $\mathcal{X}$ принадлежит смежному классу, который задаётся синдромом $\mathcal{S}$, и равномерно распределен в этом смежном классе..

Этот метод кодирования обеспечивает совершенно секретную передачу сообщения $\mathcal{S}$, если злоумышленник прослушивает не более, чем $\mu \leq n - k$ элементов вектора $\mathcal{X}$.

Перед передачей по сети источник превращает кодовый вектор $\mathcal{X}$ в кодовую матрицу $\mathbf{X}$ размера $n \times m$ над базовым полем $\mathbb{F}_q$. Для этого снова используется базис $\boldsymbol{\Omega}$.

2.4.4 Совершенная несвязываемость

Каждый промежуточный узел должен обеспечить совершенную несвязываемость полученного и отправляемого сообщения. Пусть узел получил сообщение $\mathcal{X}^{in}$ и отправил соответствующее ему сообщение $\mathcal{X}^{out}$. Злоумышленник получает $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in}$ и $\mathcal{W}^{out} = \mathbf{B}^{out}\mathcal{X}^{out}$. Должно

выполняться

$$I(\mathcal{W}^{in};\mathcal{W}^{out}|\mathcal{S})=0. \tag{2.10}$$

Рассмотрим вектор

$$\mathcal{X}^{out}=\mathcal{X}^{in}+\mathbf{G}^{\top}\mathcal{V}'=\mathbf{P}^{\top}\mathcal{S}+\mathbf{G}^{\top}(\mathcal{V}+\mathcal{V}'), \tag{2.11}$$

где $\mathcal{V}'$ равномерно распределен на $\mathbb{F}_{q^m}^{n-k}$ и не зависит от $\mathcal{X}$. Вектор $\mathcal{X}^{out}$ принадлежит смежному классу, задаваемому $\mathcal{S}$, то есть передаёт ту же информацию что и $\mathcal{X}^{in}$.

Лемма 2.2 ([66]). *Пусть x и y – независимые случайные величины, заданные на конечном поле. Если x имеет равномерное распределение, то $z=x+y$ также имеет равномерное распределение и не зависит от y.*

Тогда справедлива

Теорема 2.8. *При заданном $\mathcal{S}$ вектор $\mathcal{X}^{out}$ равномерно распределен и не зависит от $\mathcal{X}^{in}$.*

Доказательство. Необходимо показать, что $H(\mathcal{X}^{out}|\mathcal{S}\mathcal{X}^{in})=H(\mathcal{X}^{out}|\mathcal{S})=n-k$. В [9] показано, что $H(\mathcal{X}^{in}|\mathcal{S})=n-k$. Аналогично можно показать, что $H(\mathcal{X}^{out}|\mathcal{S})=n-k$. Теперь покажем, что $H(\mathcal{X}^{out}|\mathcal{S}\mathcal{X}^{in})=n-k$. Пусть $\mathbb{X}_{s,v}=\{\mathbf{T}\begin{pmatrix}s\\v\end{pmatrix}|s\in\mathbb{F}_{q^m}^{k},v\in\mathbb{F}_{q^m}^{n-k}\}$. Так как $\mathbf{T}$– матрица полного ранга, то $|\mathbb{X}_{s,v}|=q^{m(n-\mathrm{Rk}(\mathbf{T}))}=1$. Пусть $\mathbb{V}_{s,x}=\{v\in\mathbb{F}_{q^m}^{n-k}|\mathbf{T}\begin{pmatrix}s\\v\end{pmatrix}=x,s\in\mathbb{F}_{q^m}^{k},\ x\in\mathbb{F}_{q^m}^{n}\}$. Тогда $|\mathbb{V}_{s,x}|=1$.

$$\begin{aligned}H(\mathcal{X}^{in}\mathcal{X}^{out}\mathcal{V}\mathcal{V}'|\mathcal{S})&=\underset{=H(\mathcal{V})=n-k}{H(\mathcal{V}|\mathcal{S})}+\underset{=H(\mathcal{V}')=n-k}{H(\mathcal{V}'|\mathcal{S}\mathcal{V})}+\underset{\leq\log_{q^m}|\mathbb{X}_{s,v}|=0}{H(\mathcal{X}^{in}|\mathcal{S}\mathcal{V}\mathcal{V}')}+\underset{\leq\log_{q^m}|\mathbb{X}_{s,v}|=0}{H(\mathcal{X}^{out}|\mathcal{S}\mathcal{V}\mathcal{V}'\mathcal{X}^{in})}\\&=\underset{=n-k}{H(\mathcal{X}^{in}|\mathcal{S})}+H(\mathcal{X}^{out}|\mathcal{S}\mathcal{X}^{in})+\underset{\leq\log_{q^m}|\mathbb{V}_{s,x}|=0}{H(\mathcal{V}|\mathcal{S}\mathcal{X}^{in}\mathcal{X}^{out})}+\underset{=0}{H(\mathcal{V}'|\mathcal{V}\mathcal{S}\mathcal{X}^{in}\mathcal{X}^{out})}.\\H(\mathcal{X}^{out}|\mathcal{S}\mathcal{X}^{in})&=n-k.\end{aligned}$$

■

Таким образом, выполняется

$$I(\mathcal{X}^{in};\mathcal{X}^{out}|\mathcal{S})=0. \tag{2.12}$$

Лемма 2.3. *Пусть вектор $\mathcal{X}\in\mathbb{F}_{q^m}^{n}$ равномерно распределен при заданном $\mathcal{S}\in\mathbb{F}_{q^m}^{k}$, то есть $H(\mathcal{X}|\mathcal{S})=n-k$, и пусть над $\mathbb{F}_q$ задана $\mu\times n$ матрица $\mathbf{B}$ ранга μ, причем $\mu\leq n-k$. Тогда вектор $\mathbf{B}\mathcal{X}$ имеет равномерное распределение при заданном $\mathcal{S}$.*

Доказательство. Пусть $\mathcal{X}=\begin{pmatrix}x_1 & x_2 & \dots & x_n\end{pmatrix}^{\top}$. Не уменьшая общности, можно считать, что определяемые с помощью $\mathcal{S}$ элементы вектора $\mathcal{X}$ – это k последних элементов вектора. Матрицу

$\mathbf{B}$ можно представить в виде $\mathbf{B} = \begin{pmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{pmatrix}$, где $\mathbf{B}_1 \in \mathbb{F}_q^{\mu\times\mu},\ \mathbf{B}_2 \in \mathbb{F}_q^{\mu\times(n-\mu)}$, причем $\det\mathbf{B}_1 \neq 0$. Пусть $\mathbf{B}\mathcal{X} = w$.

$$\mathbf{B}\mathcal{X} = \begin{pmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{pmatrix}\mathcal{X} = \mathbf{B}_1\begin{pmatrix}x_1\\ \vdots \\ x_\mu\end{pmatrix} + \mathbf{B}_2\begin{pmatrix}x_{\mu+1}\\ \vdots \\ x_n\end{pmatrix} = w.$$

$$\begin{pmatrix}x_1\\ \vdots \\ x_\mu\end{pmatrix} = \mathbf{B}_1^{-1}w - \mathbf{B}_1^{-1}\mathbf{B}_2\begin{pmatrix}x_{\mu+1}\\ \vdots \\ x_n\end{pmatrix}.$$

Из последних $n-\mu-k$ элементов вектора $\mathcal{X}$ при фиксированном w и заданном $\mathcal{S}$ можно получить первые μ элементов. Тогда $P(\mathbf{B}\mathcal{X} = w|\mathcal{S}) = \frac{q^{m(n-\mu-k)}}{q^{m(n-k)}}$, где $q^{m(n-k)}$ – общее число исходов, равное количеству способов, которыми можно задать вектор $\mathcal{X}$ при заданном $\mathcal{S}$, а $q^{m(n-\mu-k)}$ – число «успешных» исходов, равное количеству способов, которыми можно задать последние $n-\mu-k$ элементов вектора $\mathcal{X}$ при заданном $\mathcal{S}$. Следовательно, $P(\mathbf{B}\mathcal{X} = w|\mathcal{S}) = \frac{1}{q^{m\mu}},\ \forall w \in \mathbb{F}_{q^m}^{\mu}$. Более того, из последнего соотношения следует, что вектор $\mathbf{B}\mathcal{X}$ не зависит от $\mathcal{S}$. ■

Теорема 2.9. *Пусть $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in},\ \mathcal{W}^{out} = \mathbf{B}^{out}\mathcal{X}^{out}$, векторы $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ равномерно распределены и независимы при заданном $\mathcal{S} \in \mathbb{F}_{q^m}^k$, $\mathbf{B}^{in}, \mathbf{B}^{out} \in \mathbb{F}_q^{\mu\times n}$, $\mathrm{Rk}\mathbf{B}^{in} = \mathrm{Rk}\mathbf{B}^{out} = \mu,\ \mu \leq n-k$. Тогда векторы $\mathcal{W}^{in}$ и $\mathcal{W}^{out}$ независимы при заданном $\mathcal{S}$.*

Доказательство. По лемме 2.3 векторы $\mathcal{W}^{in}$ и $\mathcal{W}^{out}$ имеют равномерное распределение. Рассмотрим вектор

$$\mathcal{U} = \begin{pmatrix}\mathcal{W}^{in}\\ \mathcal{W}^{out}\end{pmatrix} = \begin{pmatrix}\mathbf{B}^{in} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}^{out}\end{pmatrix}\begin{pmatrix}\mathcal{X}^{in}\\ \mathcal{X}^{out}\end{pmatrix}.$$

$$\mathrm{Rk}\begin{pmatrix}\mathbf{B}^{in} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}^{out}\end{pmatrix} = \mathrm{Rk}\mathbf{B}^{in} + \mathrm{Rk}\mathbf{B}^{out} = 2\mu.$$

Векторы $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ равномерно распределены и независимы при заданном $\mathcal{S}$, то есть $2k$ элементов вектора $\begin{pmatrix}\mathcal{X}^{in} & \mathcal{X}^{out}\end{pmatrix}^\top$ фиксированы, а $2(n-k)$ элементов равномерно распределены в поле $\mathbb{F}_{q^m}$. Тогда по лемме 2.3 $P(\mathcal{U} = u|\mathcal{S}) = \frac{1}{q^{2m\mu}}$, то есть вектор $\mathcal{U}$ имеет равномерное распределение, и следовательно, векторы $\mathcal{W}^{in}$ и $\mathcal{W}^{out}$ независимы. ■

Таким образом, из теорем 2.8 и 2.9 следует соотношение (2.10).

В общем случае любой i-й промежуточный узел маршрута, получивший сообщение $\mathcal{Y}^{in} = \mathbf{A}_i X^{in}$, может построить сообщение для дальнейшей передачи узлу j как

$$\mathcal{Y}^{out} = \mathbf{A}_{i-j}\mathbf{A}_i\mathcal{X}^{out} = \mathbf{A}_{i-j}\mathbf{A}_i(\mathcal{X}^{in} + \mathbf{G}^\top\mathcal{V}_i') = \mathbf{A}_{i-j}(\mathcal{Y}^{in} + \mathbf{A}_i\mathbf{G}^\top\mathcal{V}_i'),$$

где $\mathcal{V}_j' \in \mathbb{F}_{q^m}^{(n-k)}$ выбирается произвольно промежуточным узлом. Эта процедура выполняется только на узлах маршрута, то есть на узлах r_1 и r_2 (рис. 2.3). Узлы a и b не преобразуют

принятые сообщения по правилу (2.11). Таким образом, злоумышленник может проследить сообщение от источника s до первого промежуточного узла r_1. Узел r_1 уже отправит сообщение, совершенно несвязываемое с принятым.

2.5 Активный злоумышленник

В пункте 2.4 рассматривалась схема анонимной передачи для пассивного злоумышленника. Теперь рассмотрим случай, когда злоумышленник является активным и может не только прослушивать пакеты, но и вставлять ограниченное число своих пакетов. Будем рассматривать пассивного злоумышленника, описанного в пункте 2.4.2, который дополнительно может вставить не более t своих пакетов. Этим злоумышленник может повредить передачу верного сообщения получателю. Пакеты, вставляемые злоумышленником, можно рассматривать как ошибки, происходящие во время передачи. Таким образом, действия активного злоумышленника в сети, где данные передаются без ошибок, можно рассматривать как действия пассивного злоумышленника в сети с ошибками. Тогда в качестве модели злоумышленника примем модель пассивного злоумышленника из пункта 2.4.2, а к модели сети (п. 2.4.1) добавим условие, что в сети может произойти не более t ошибок. Опишем способ кодирования источника для этого случая.

2.5.1 Кодирование источника для передачи с ошибками

В случае безошибочной передачи все множество $\{0,1\}^n$ заполнялось смежными классами выбранного кода. Для того чтобы обеспечить исправление ошибок точки различных смежных классов должны быть разнесены на большее расстояние. Авторы работы [67] предложили для этого разбивать на смежные классы не все множество, а подмножество и представили схему вложенных кодов. Пусть C_1 – линейный (n, k_1) код, а C_2 – (n, k_2) код, где $k_1 > k_2$ и $C_2 \subset C_1$, то есть каждое кодовое слово C_2 является одновременно и кодовым словом C_1. Порождающие матрицы $\mathbf{G}_1$, $\mathbf{G}_2$ и проверочные матрицы $\mathbf{H}_1$, $\mathbf{H}_2$ кодов C_1 и C_2, соответственно, связаны соотношениями

$$\mathbf{G}_1 = \begin{pmatrix} \Delta\mathbf{G}_1 \\ \mathbf{G}_2 \end{pmatrix}, \quad \mathbf{H}_2 = \begin{pmatrix} \mathbf{H}_1 \\ \Delta\mathbf{H} \end{pmatrix},$$

где $\Delta\mathbf{G}_1$ и $\Delta\mathbf{H}$ – $(k_1 - k_2) \times n$ матрицы. Синдромы некоторого вектора $\mathcal{X}$ связаны соотношением

$$\mathcal{S}_2 = \mathbf{H}_2\mathcal{X} = \begin{pmatrix} \mathbf{H}_1 \\ \Delta\mathbf{H} \end{pmatrix} \mathcal{X} = \begin{pmatrix} \mathbf{H}_1\mathcal{X} \\ \Delta\mathbf{H}\mathcal{X} \end{pmatrix} = \begin{pmatrix} \mathcal{S}_1 \\ \mathcal{S} \end{pmatrix}.$$

Если $\mathcal{X} \in C_1$, то $\mathcal{S}_1 = 0$ и $\mathcal{S}_2 = \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$. Вектор $\mathcal{S}$, который называют относительным синдромом, имеет длину $k_1 - k_2$. Если коды C_1 и C_2 заданы над полем $\mathbb{F}_{q^m}$, то код C_1 можно разбить на

$q^{m(k_1-k_2)}$ смежных классов C_2, варьируя $\mathcal{S}$. Это использовано в методе секретной передачи Силвы и Кшишанга для сетевого кодирования с ошибками [68]. В качестве кода C_1 выбирается $(n, k+\mu)$ MPP код с порождающей матрицей $\mathbf{G}_1 \in \mathbb{F}_{q^m}^{(k+\mu)\times n}$. Кодовое сообщение выражается как $\mathcal{X} = \mathbf{G}_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix}$, где $\mathcal{S} \in \mathbb{F}_{q^m}^k$ – информационное сообщение, а $\mathcal{V} \in \mathbb{F}_{q^m}^\mu$ – равномерно распределённый вектор, независимый от $\mathcal{S}$. Сообщение $\mathcal{S}$ может быть передано совершенно секретно при прослушивании μ пакетов сообщения $\mathcal{X}$, если $\mathcal{S}$ – это относительный синдром. Так как длина $\mathcal{S}$ равна k, то должен быть (n, μ) MPP код C_2, вложенный в C_1. Тогда последние μ строк матрицы $\mathbf{G}_1$ должны образовывать порождающую матрицу $\mathbf{G}_2$ кода C_2, то есть $\mathbf{G}_1 = \begin{pmatrix} \Delta\mathbf{G}_1 \\ \mathbf{G}_2 \end{pmatrix}$. Это условие выполнено для MPP кода, порождающая матрица которого имеет вид (2.4). Пусть $\mathbf{T}^\top = \begin{pmatrix} \Delta\mathbf{G} \\ \mathbf{G}_1 \end{pmatrix}$ – невырожденная $n \times n$ матрица. Тогда

$$\mathcal{X} = \mathbf{G}_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix} = \mathbf{T} \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix} = \begin{pmatrix} \Delta\mathbf{G}^\top & \Delta\mathbf{G}_1^\top & \mathbf{G}_2^\top \end{pmatrix} \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix} = \begin{pmatrix} \Delta\mathbf{G}^\top & \Delta\mathbf{G}_1^\top \end{pmatrix} \mathcal{S}' + \mathbf{G}_2^\top \mathcal{V},$$

где $\mathcal{S}' = \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$ – синдром кода C_2 и $\mathbf{G}_2^\top \mathcal{V}$ – случайный вектор кода C_2. Тогда $\mathcal{X}$ – это случайный вектор смежного класса кода C_2 с синдромом $\mathcal{S}'$.

При возникновении ошибок сообщение, полученное некоторым промежуточным узлом, может быть выражено как $\mathcal{Y} = \mathbf{A}\mathcal{X} + \mathbf{D}\mathcal{Z}$, где $\mathcal{X}$ – передаваемое сообщение, $\mathbf{A} \in \mathbb{F}_q^{n\times n}$ – матрица передачи, $\mathcal{Z} \in \mathbb{F}_{q^m}^t$ – вектор ошибочных пакетов, $\mathbf{D} \in \mathbb{F}_q^{n\times t}$ – матрица передачи ошибочных пакетов. Исправление ошибок зависит от корректирующих способностей кода C_1. Ошибки в количестве t могут быть исправлены, если ранговое расстояние кода C_1 удовлетворяет условию $d(C_1) \geq 2t + 1$.

2.5.2 Совершенная несвязываемость

Покажем, что вредоносные пакеты злоумышленника не нарушают несвязываемости сообщений. Рассмотрим вектор

$$\mathcal{X}^{out} = \mathcal{X}^{in} + \mathbf{G}_2^\top \mathcal{V}' = \begin{pmatrix} \Delta\mathbf{G}^\top & \Delta\mathbf{G}_1^\top \end{pmatrix} \mathcal{S}' + \mathbf{G}_2^\top (\mathcal{V} + \mathcal{V}'), \tag{2.13}$$

где $\mathcal{V}'$ – равномерно распределённый на $\mathbb{F}_{q^m}^\mu$ вектор, независимый от $\mathcal{X}^{in}$. Вектор $\mathcal{X}^{out}$ принадлежит тому же смежному классу, что и $\mathcal{X}^{in}$. По теореме 2.8

$$H(\mathcal{X}^{out}|\mathcal{X}^{in}\mathcal{S}') = H(\mathcal{X}^{out}|\mathcal{S}') = \mu.$$

Рассмотрим i-й промежуточный узел. Пусть злоумышленник прослушал μ входящих соединений этого узла, получив $\mathcal{W}^{in} = \mathbf{B}^{in}\mathcal{X}^{in}$, а на других входных соединениях вставил ошибки

$\mathcal{Z} \in \mathbb{F}_{q^m}^t$. Тогда узел получил сообщение

$$\mathcal{Y}^{in} = \mathbf{A}_i \mathcal{X}^{in} + \mathbf{D}_i \mathcal{Z},$$

$\mathbf{A}_i$ – матрица передачи от источника до узла i, $\mathbf{D}_i$ – матрица передачи ошибочных пакетов. Следующему промежуточному узлу j узел i отправит

$$\mathcal{Y}^{out} = \mathbf{A}_{i-j}(\mathbf{A}_i \mathcal{X}^{out} + \mathbf{D}_i \mathcal{Z}) = \mathbf{A}_{i-j}(\mathbf{A}_i(\mathcal{X}^{in} + \mathbf{G}_2^\top \mathcal{V}') + \mathbf{D}_i \mathcal{Z}) = \mathbf{A}_{i-j}(\mathcal{Y}^{in} + \mathbf{A}_i \mathbf{G}_2^\top \mathcal{V}').$$

$\mathcal{W}^{in}$ можно представить как $\mathcal{W}^{in} = \mathbf{E}^{in} \mathbf{A}_i \mathcal{X}^{in}$, где $\mathbf{E}^{in}$ – матрица размера $\mu \times n$ и ранга μ, определяющая какие координаты $\mathbf{A}_i \mathcal{X}^{in}$ прослушал злоумышленник. $\mathbf{E}^{in} = (e_{kl})$, где

$$e_{kl} = \begin{cases} 1, \text{ если координата } l \text{ прослушана и } e_{kr} = 0 \ \forall r \neq l, \ e_{tl} = 0 \ \forall t \neq k, \\ 0, \text{ иначе.} \end{cases}$$

Например, пусть

$$\mathbf{A}_i \mathcal{X}^{in} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

а злоумышленник подслушал

$$\mathcal{W}^{in} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 \end{pmatrix}.$$

Тогда

$$\mathbf{E}^{in} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Прослушав μ выходных соединений, злоумышленник получил $\mathcal{W}^{out} = \mathbf{E}^{out} \mathcal{Y}^{out}$, где $\mathbf{E}^{out}$ определяется аналогично $\mathbf{E}^{in}$. Тогда по теореме 2.9

$$I(\mathcal{W}^{in}; \mathcal{W}^{out} | \mathcal{S}') = 0,$$

если

$$I(\mathbf{A}_i \mathcal{X}^{in}; \mathbf{A}_{i-j}(\mathcal{Y}^{in} + \mathbf{A}_i \mathbf{G}_2^\top \mathcal{V}') | \mathcal{S}') = 0.$$

Лемма 2.4 (Лемма 7.1 [69]). *Пусть для тройки случайных величин $\{X, Y, Z\}$ выполняется одно из ниже перечисленных условий:*

1. $P_{Z|XY}(z|x, x) = P_{Z|Y}(z|y)$ *для всех значений* x.
2. $H(X|YZ) = H(X|Y)$.

Условия 1 и 2 эквивалентны. Выполнение одного их них влечёт за собой выполнение другого.

Обозначим $X = \mathbf{A}_i\mathcal{X}^{in}$, $Y = \mathcal{Y}^{in} + \mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'$, $Z = \mathbf{A}_{i-j}(\mathcal{Y}^{in} + \mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}')$. Покажем, что $H(X|ZY) = H(X|Y)$.

$$\begin{aligned} H(ZYX) &= H(Y) + H(Z|Y) + H(X|ZY) \\ &= H(Y) + H(X|Y) + H(Z|XY) \end{aligned} \tag{2.14}$$

Пусть $\mathbb{Z}_Y = \{\mathbf{A}_{i-j}y | y \in \mathbb{F}_{q^m}^n\}$. Тогда $|\mathbb{Z}_Y| = q^{m(n-\mathrm{Rk}A_{i-j})} = 1$, так как $\mathrm{Rk}\mathbf{A}_{i-j} = n$. Из соотношения (2.14) следует, что

$$\underbrace{H(Z|Y)}_{\leq \log_{q^m}|\mathbb{Z}_Y|=0} + H(X|ZY) = H(X|Y) + \underbrace{H(Z|XY)}_{\leq H(Z|Y)=0}$$

$$H(X|ZY) = H(X|Y)$$

По лемме 2.4 тройка случайных величин $\{X, Y, Z\}$ образует цепь Маркова.

Лемма 2.5 (Лемма об обработке сигнала, Лемма 7.2 [69])**.** *Если случайные величины* $\{X, Y, Z\}$ *образуют цепь Маркова, то*

$$I(Z;X) \leq I(Z;Y);$$
$$I(Z;X) \leq I(Y;X).$$

По лемме об обработке сигнала

$$I(\mathbf{A}_i\mathcal{X}^{in}; \mathbf{A}_{i-j}(\mathcal{Y}^{in}+\mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}')|\mathcal{S}') \leq I(\mathbf{A}_i\mathcal{X}^{in}; \mathcal{Y}^{in}+\mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'|\mathcal{S}') = I(\mathbf{A}_i\mathcal{X}^{in}; \mathbf{A}_i\mathcal{X}^{in}+\mathbf{D}_i\mathcal{Z}+\mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'|\mathcal{S}').$$

Матрица $\mathbf{A}_i$ задана над $\mathbb{F}_q$, её ранг равен n. Матрица $\mathbf{G}_2$ – подматрица порождающей матрицы МРР кода (2.4), она задана над $\mathbb{F}_{q^m}$. Её строки и столбцы линейно независимы над $\mathbb{F}_q$. Следовательно, строковый ранг $\mathbf{G}_2$ над $\mathbb{F}_q$ равен μ, а столбцевой ранг равен n. Строки матрицы $\mathbf{A}_i\mathbf{G}_2^\top$ представляют собой линейные комбинации строк $\mathbf{G}_2^\top$. Таким образом, строковый ранг матрицы $\mathbf{A}_i\mathbf{G}_2^\top$ над $\mathbb{F}_q$ равен n. Так как $\mu \leq n$, то μ компонент вектора $\mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'$ независимы и равномерно распределены в $\mathbb{F}_{q^m}$, то есть $P(\mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'|\mathcal{S}') = \frac{1}{q^{m\mu}}$. По теореме 2.8 вектор $\mathbf{A}_i\mathcal{X}^{in} + \mathbf{D}_i\mathcal{Z} + \mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'$ равномерно распределен при заданном $\mathcal{S}'$ независимо от распределения ошибочных пакетов $\mathcal{Z}$ и не зависит от $\mathbf{A}_i\mathcal{X}^{in}$. Тогда

$$I(\mathbf{A}_i\mathcal{X}^{in}; \mathbf{A}_i\mathcal{X}^{in} + \mathbf{D}_i\mathcal{Z} + \mathbf{A}_i\mathbf{G}_2^\top\mathcal{V}'|\mathcal{S}') = 0,$$

и следовательно по теореме 2.9

$$I(\mathcal{W}^{in}; \mathcal{W}^{out}|\mathcal{S}') = 0.$$

Таким образом, идея метода для пассивного злоумышленника обобщается на случай активного злоумышленника. Далее будем рассматривать только пассивного злоумышленника.

2.6 Совершенная несвязываемость сообщений для традиционной маршрутизации

В этом разделе диссертационной работы показано как можно применить к сетям с традиционной маршрутизацией теоретико-информационный метод обеспечения несвязываемости.

2.6.1 Модель сети

Сеть представляется графом $G(V, E)$, вершины V которого есть узлы сети, а ребра E – соединения. В сети присутствуют N источников сообщений и L получателей, между которыми возможны как одноадресные, так и многоадресные передачи. Во время передачи возможно возникновение ошибок. Сообщения, передаваемые в сеть, состоят из пакетов, которые являются элементами поля $\mathbb{F}_q$.

Предполагается, что маршрутная информация не распространяется в открытом доступе. Маршрут может быть сформирован таким образом, что узлы, не участвующие в передаче, не обладают о нём никакой информацией. Промежуточные узлы маршрута обладают информацией только о своих ближайших соседях.

2.6.2 Модель злоумышленника

Рассматривается пассивный локальный внешний адаптивный злоумышленник. Локальность злоумышленника состоит в том, что он не может прослушивать все пакеты сообщения, поступающего в некоторый узел, и все пакеты сообщения, отправляемого этим узлом. Злоумышленник может прослушивать не более, чем μ пакетов входящего сообщения и не более μ пакетов выходящего. Как на практике может быть реализован такой злоумышленник? В отличие от сетевого кодирования при традиционной маршрутизации все пакеты сообщения часто передаются по одному и тому же пути, то есть по одному и тому же набору соединений. Тогда если злоумышленник имеет доступ к какому-то соединению, то он может прослушать все пакеты, проходящие через него. Но теоретико-информационный подход накладывает физические ограничения на злоумышленника. Прослушивая какое-то соединение сети, злоумышленник делает отводное соединение к своему устройству. Злоумышленник может не получить всех пакетов, если скорость передачи превышает скорость его соединения, или устройство злоумышленника не имеет достаточно памяти, чтобы принять и обработать все пакеты.

2.6.3 Кодирование источника

В стандартах 100 гигабитного Ethernet для исправления ошибок используется код Рида-Соломона. Порождающая матрица $(n, k+\mu)$ кода Рида-Соломона имеет вид

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k+\mu-1} & \alpha_2^{k+\mu-1} & \dots & \alpha_n^{k+\mu-1} \end{pmatrix},$$

где $\alpha_i \in \mathbb{F}_q,\ i = 1, 2, \dots, n$. Последние μ строк формируют порождающую матрицу (n, k) кода Рида-Соломона. Это позволяет использовать метод кодирования смежными классами [68], рассмотренный в пункте 2.5.1, для кодов Рида-Соломона.

Пусть C_1 – $(n, k+\mu)$ код Рида-Соломона с порождающей матрицей $\mathbf{G}_1$, заданный над $\mathbb{F}_q$, а C_2 – (n, k) код Рида-Соломона с порождающей матрицей $\mathbf{G}_2$, заданный над тем же полем, $C_2 \subset C_1$. Информационное сообщение $\mathcal{S} \in \mathbb{F}_q^k$ кодируется следующим образом $\mathcal{X} = \mathbf{G}_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix}$, где $\mathcal{V} \in \mathbb{F}_q^\mu$. Пусть задана невырожденная матрица $\mathbf{T}^\top = \begin{pmatrix} \Delta\mathbf{G} \\ \mathbf{G}_1 \end{pmatrix}$. Так как $C_2 \subset C_1$, то $\mathbf{G}_1 = \begin{pmatrix} \Delta\mathbf{G}_1 \\ \mathbf{G}_2 \end{pmatrix}$. Тогда

$$\mathcal{X} = \mathbf{G}_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix} = \mathbf{T} \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix} = \begin{pmatrix} \Delta\mathbf{G}^\top & \Delta\mathbf{G}_1^\top & \mathbf{G}_2^\top \end{pmatrix} \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix} = \begin{pmatrix} \Delta\mathbf{G}^\top & \Delta\mathbf{G}_1^\top \end{pmatrix} \mathcal{S}' + \mathbf{G}_2^\top \mathcal{V},$$

где $\mathcal{S}' = \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$ – синдром кода C_2 и $\mathbf{G}_2^\top \mathcal{V}$ – случайный вектор кода C_2. Тогда $\mathcal{X}$ – это случайный вектор смежного класса кода C_2 с синдромом $\mathcal{S}'$. Сообщение $\mathcal{S}$ передаётся совершенно секретно, если злоумышленник прослушивает не более, чем μ элементов $\mathcal{X}$. Исправление ошибок зависит от корректирующих способностей кода C_1. Количество исправляемых ошибок t, количество секретно переданных пакетов k и количество подслушанных злоумышленником пакетов μ связаны следующим образом

$$\mu \le n - k - 2t.$$

2.6.4 Совершенная несвязываемость

Совершенная несвязываемость достигается так же, как и в случае сетевого кодирования и определяется соотношением (2.13) с той лишь разницей, что все векторы в (2.13) рассматриваются над полем $\mathbb{F}_q$. Заметим, что теоремы 2.8, 2.9 верны и в том случае, когда векторы $\mathcal{X}^{in}, \mathcal{X}^{out}, \mathcal{S}'$ рассматриваются над полем $\mathbb{F}_q$.

В общем случае i-промежуточный узел получает $\mathcal{Y}^{in} = \mathcal{X}^{in} + \mathcal{Z}$, где $\mathcal{Z}$ – вектор ошибочных пакетов. А отправляет $\mathcal{Y}^{out} = \mathcal{Y}^{in} + \mathbf{G}_2^\top \mathcal{V}' = \mathcal{X}^{out} + \mathcal{Z}$. По теореме 2.8

$$I(\mathcal{Y}^{out}; \mathcal{Y}^{in} | \mathcal{S}') = 0. \tag{2.15}$$

На входном соединении этого узла злоумышленник подслушает $\mathcal{W}^{in} = \mathbf{E}^{in}\mathcal{Y}^{in}$, где E^{in} – $\mu \times n$ матрица, которая определяется так же, как и в пункте 2.5.2. На выходном соединении этого узла злоумышленник подслушает $\mathcal{W}^{out} = \mathbf{E}^{out}\mathcal{Y}^{out}$. По теореме 2.9

$$I(\mathcal{W}^{out}; \mathcal{W}^{in} | \mathcal{S}').$$

2.7 Анализ

2.7.1 Стойкость

Проанализируем стойкость метода в случае сетевого кодирования.

Секретность передаваемых сообщений является необходимым условием несвязываемости. Рассмотрим следующую атаку. Напомним, что по сети передаются матрицы, заданные над полем $\mathbb{F}_q$. Пусть злоумышленник прослушал сообщение $\mathbf{X}^{in} \in \mathbb{F}_q^{n \times m}$, поступающее в некий промежуточный узел, и одно из отправляемых этим узлом сообщений $\mathbf{X}^{out} \in \mathbb{F}_q^{n \times m}$. Если эти матрицы состоят из пакетов одного и того же источника, то синдромы соответствующих им кодовых векторов должны совпадать. Это позволяет установить связь между сообщениями, несмотря на условие (2.12). Предположим, что злоумышленнику не известен базис $\mathbf{\Omega}$. Злоумышленник выбирает некий базис $\mathbf{\Omega}' = \mathbf{\Omega}\mathbf{Q}$, где $\mathbf{Q}$ – невырожденная матрица размера $m \times m$, и сравнивает синдромы $\mathbf{H}\mathbf{X}^{in}\mathbf{\Omega}'^\top$ и $\mathbf{H}\mathbf{X}^{out}\mathbf{\Omega}'^\top$. Если базис подобран верно, то синдромы будут равны, из чего злоумышленник может сделать вывод, что сообщения $\mathbf{X}^{in}$ и $\mathbf{X}^{out}$ принадлежат одному и тому же сеансу связи. В общем случае при $\mathbf{Q} \neq \mathbf{I}_m$, где $\mathbf{I}_m$ – единичная матрица порядка m, выполняется

$$\mathbf{H}(\mathbf{X}^{in} - \mathbf{X}^{out})\mathbf{Q}^\top\mathbf{\Omega}^\top \neq 0.$$

Таким образом, в случае глобального злоумышленника анонимности нельзя достичь без использования секретного ключа, который должен быть известен источнику и получателю. Ключом в данном случае является базис. Количество базисов размера m в поле $\mathbb{F}_q$ составляет $q^m(q^m - q)(q^m - q^2)\dots(q^m - q^{m-1})$.

В случае локального злоумышленника подобная атака не будет успешной как для случая сетевого кодирования, так и для случая традиционной маршрутизации благодаря секретности синдрома $I(\mathcal{S}; \mathcal{W}^{in}) = I(\mathcal{S}; \mathcal{W}^{out}) = 0$. Скорость анонимной передачи составляет $\frac{k}{n}$. Совершенная несвязываемость возможна для любого $k < n$, если выполняется $\mu \leq n - k$.

Несвязываемость сообщений, обеспечиваемую шифрованием, трудно оценить с помощью взаимной информации, так как практически применяемые шифры являются семантически секретными, а семантическая секретность не предполагает простого условия на взаимную информацию. Чтобы понять местоположение предлагаемого в этой главе метода среди других методов воспользуемся следующей интерпретацией, помогающей сопоставить совершенную и семантическую секретности. Пусть g задаёт преобразование $\mathcal{X}^{in}$ в $\mathcal{X}^{out}$, $g : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^{n-k} \to \mathbb{F}_{q^m}^n$. Совершенная несвязываемость означает, что распределение выходного сообщения, полученного преобразованием некоторого $\mathcal{X}_1^{in}$ с помощью некоторого $\mathcal{V}'$, совпадает с распределением выходного сообщения, полученного преобразованием некоторого другого $\mathcal{X}_2^{in}$ с помощью $\mathcal{V}'$, то есть $P(g(\mathcal{X}_1^{in}, \mathcal{V}') = \mathcal{X}^{out}) = P(g(\mathcal{X}_2^{in}, \mathcal{V}') = \mathcal{X}^{out})\ \forall \mathcal{X}_1^{in}, \mathcal{X}_2^{in}, \mathcal{V}', \mathcal{X}^{out}$. Для систем, основанных на шифровании, таких так Mix-net, Tor, g задает алгоритм шифрования $g : \mathbb{X}^{in} \times \mathbb{K} \to \mathbb{X}^{out}$, где $\mathbb{X}^{in}$– множество входных сообщений, $\mathbb{X}^{in}$– множество выходных сообщений и $\mathbb{K}$–множество ключей. Неформально семантическую секретность можно описать таким образом: имея $g(\mathcal{X}^{in}, \mathcal{K})$, злоумышленник не может оценить $\mathcal{X}^{in}$ лучше, чем если бы он просто угадывал $\mathcal{X}^{in}$ без $g(\mathcal{X}^{in}, \mathcal{K})$. Более формально шифр g является семантически секретным, когда распределения $P(g(\mathcal{X}_1^{in}, \mathcal{K}) = \mathcal{X}^{out})$ и $P(g(\mathcal{X}_2^{in}, \mathcal{K}) = \mathcal{X}^{out})$ нельзя отличить за полиномиальное время, то есть используя алгоритм полиномиальной сложности, для любых конкретных $\mathcal{X}_1^{in}, \mathcal{X}_2^{in}$. Это еще раз подчеркивает главное отличие предлагаемого метода от всех предыдущих – рассматривается теоретико-информационная модель несвязываемости вместо модели, основанной на вычислительной сложности. Как показано выше, это верно только для локального злоумышленника. В случае глобального злоумышленника возникает необходимость в ключе, которым является базис расширенного поля, следовательно размер ключа в битах может быть довольно большим, и модель превращается в вычислительную. Она основана на сложности подбора базиса.

2.7.2 Сложность

Оценим сложность предлагаемого метода для сетевого кодирования. Он состоит из нескольких процедур.

1. Приведение полученного сообщения к векторной форме $\mathcal{Y}^{in} = \mathbf{Y}^{in}\mathbf{\Omega}^{\top}$.
2. Генерирование случайного вектора $\mathcal{V}'$ над полем $\mathbb{F}_{q^m}$ длины $n-k$ в случае пассивного злоумышленника и длины μ в случае активного.
3. Кодирование вектора $\mathcal{V}'$ в вектор $\mathcal{Q}$ с использованием MPP кода.
4. Вычисление выходного сообщения $\mathcal{Y}^{out} = \mathcal{Y}^{in} + \mathbf{A}_i\mathcal{Q}$. Здесь не учитывается умножение на матрицу передачи $\mathbf{A}_{i-j}$, так как это операция сетевого кодирования, а не предлагаемого метода.

5. Приведение полученного сообщения к матричной форме $\mathbf{Y}^{out} = \mathcal{Y}^{out}\mathbf{\Omega}(\mathbf{\Omega}^\top\mathbf{\Omega})^{-1}$.

Для первой процедуры понадобиться nm умножений элементов базового поля $\mathbb{F}_q$ на элементы расширенного поля $\mathbb{F}_{q^m}$, что можно оценить как $O(nm^2)$ умножений в $\mathbb{F}_q$, а также $n(m-1)$ сложений в $\mathbb{F}_{q^m}$. Окончательно эту процедуру можно оценить как $O(nm^2)$ операций в $\mathbb{F}_q$. Чтобы сгенерировать вектор $\mathcal{V}'$, нужно сгенерировать случайную матрицу $\mathbf{V}' \in \mathbb{F}_q^{h\times m}$, то есть hm случайных элементов $\mathbb{F}_q$, а затем с помощью базиса $\mathbf{\Omega}$ перейти в $\mathbb{F}_{q^m}$. В случае пассивного злоумышленника $h = n - k$, а в случае активного $h = \mu$. Для того чтобы сгенерировать случайное число, обычно генерируют случайную битовую строку соответствующей длины и конвертируют её в число. Если $q = 2^r$, то нужно сгенерировать r случайных бит. Для случая $2^r < q < 2^{r+1}$ существуют различные алгоритмы. Алгоритм, предложенный в [70], является оптимальным, то есть гарантирует, что среднее число случайных бит u, которое нужно сгенерировать, чтобы получить равномерно распределенный элемент поля минимально. Для этого алгоритма выполняется $\lceil \log_2 q \rceil < u < \lceil \log_2 q \rceil + 1$. Тогда сложность генерации матрицы $\mathbf{V}'$ можно оценить как $O(hm)$ битовых операций при условии, что q фиксировано. Сложность перехода в расширенное поле $\mathcal{V}' = \mathbf{V}'\mathbf{\Omega}^\top$ оценивается аналогично первой процедуре как $O(hm^2)$ операций в $\mathbb{F}_q$. Кодирование (n, h) МРР кода может быть выполнено с помощью $2hnm$ сложений в $\mathbb{F}_q$ при использовании нормального базиса $\mathbf{\Omega}$, т.е. базиса вида $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$, где $\alpha \in \mathbb{F}_{q^m}$ [71]. Третья процедура состоит из двух – умножение матрицы $\mathbf{A}_i$ на вектор $\mathcal{Q}$, что может быть выполнено с помощью n^2m операций в $\mathbb{F}_q$, и сложение двух векторов в поле $\mathbb{F}_{q^m}$, которое выполняется за nm сложений в $\mathbb{F}_q$. Последняя процедура может быть упрощена использованием подходящего нормального базиса. Каждый промежуточный узел может предварительно вычислить $\hat{\mathbf{\Omega}} = \mathbf{\Omega}(\mathbf{\Omega}^\top\mathbf{\Omega})^{-1}$. $\hat{\mathbf{\Omega}}$ – это вектор-строка длины m, элементы которой выражаются через элементы вида $\alpha^{q^i},\ i = 0, 1, \ldots, m-1$. Для умножения элемента поля $\mathbb{F}_{q^m}$ на элемент вектор-строки $\hat{\mathbf{\Omega}}$ понадобиться $O(m)$ сложений в $\mathbb{F}_q$ [71]. Тогда последняя процедура может быть выполнена с помощью $O(nm^2)$ сложений в $\mathbb{F}_q$. Так как $n \leq m$, то доминирует сложность последней процедуры и сложность предлагаемого метода можно оценить как $O(nm^2)$ операций в $\mathbb{F}_q$.

Для метода обеспечения несвязываемости в случае традиционной маршрутизации доминирующей является операция кодирования кода Рида-Соломона, и сложность метода оценивается сложностью этой операции.

2.8 Выводы

В этой главе диссертационной работы:

1) предложен метод обеспечения несвязываемости сообщений для цифрового когерентного сетевого кодирования;

2) показано, что метод обеспечивает совершенную несвязываемость в случае пассивного и активного локальных злоумышленников;

3) предложен метод обеспечения несвязываемости сообщений для традиционной маршрутизации;

4) проведён анализ стойкости методов, приведена атака, демонстрирующая, что в случае глобального злоумышленника анонимность в теоретико-информационном смысле невозможна;

5) оценена сложность предложенных методов.

Глава 3

Анонимное аналоговое сетевое кодирование

Эта глава диссертационной работы посвящена методу анонимности для сетевого кодирования на физическом уровне [18, 21]. Предлагаемый метод основан на кодировании смежными классами для алгебраических решёток.

Прежде чем излагать суть метода приведем все сведения необходимые для его описания. В разделе 3.1 будет изложен принцип аналогового сетевого кодирования и даны необходимые понятия из теории алгебраических решеток, а в разделе 3.2 будут изложены известные результаты из теории канала с подслушиванием типа I, на основе которого строится предлагаемый метод.

3.1 Аналоговое сетевое кодирование

Главное отличие беспроводных сетей передачи данных от проводных состоит в широковещательности беспроводных сетей – сигнал, отправленный некоторым узлом, получают все узлы, находящиеся в зоне действия отправителя. Узел сети получает не только предназначенный ему сигнал, но также и другие сигналы, которые зашумляют полезный сигнал. С развитием беспроводных сетей было предложено множество алгоритмов для предотвращения интерферирования передаваемых сигналов. Часто методы борьбы с интерференцией приводят к уменьшению скорости передачи при увеличении количества узлов сети. С появлением сетевого кодирования возникла идея использовать интерферирование сигналов для сетевого кодирования на физическом уровне, что приводит к увеличению скорости передачи [72, 73]. Этот способ передачи будем называть *аналоговое сетевое кодирование*. В качестве модели беспроводного канала используют канал с аддитивным гауссовским шумом (AWGN). Более того, аддитивный шум в беспроводной сети также моделируют гауссовским шумом [74]. Известно, что коды на вложен-

ных решётках достигают пропускной способности AWGN канала [75]. Приведем необходимые сведения о решётках на основе [76].

3.1.1 Основные сведения теории решеток в евклидовом пространстве

Решётка Λ размерности n представляет собой группу, заданную на $\mathbb{R}^n$, с операцией сложения в евклидовом пространстве. Решётку можно задать с помощью порождающей матрицы. Выберем n линейно независимых векторов $g_1, g_2, \dots g_n \in \mathbb{R}^n$, которые сформируют порождающую матрицу

$$\mathbf{G} = \begin{pmatrix} g_1 & g_2 & \dots & g_n \end{pmatrix}.$$

Тогда решётка Λ – это множество всех целочисленных линейных комбинаций базисных векторов $g_1, g_2, \dots g_n$, т.е.

$$\Lambda = \{\lambda = \mathbf{G}z : z \in \mathbb{Z}^n\}.$$

Детерминантом решётки называется модуль детерминанта порождающей матрицы

$$\det(\Lambda) = |\det(\mathbf{G})|.$$

Смежный класс решётки Λ определяется как множество

$$\Lambda_x = \Lambda + x = \{\lambda + x : \lambda \in \Lambda\}$$

для любого $x \in \mathbb{R}^n$. Объединение Λ_x для все x покрывает все пространство $\mathbb{R}^n$, но это объединение имеет пересечения. Минимальное множество $\mathcal{P}_0$, удовлетворяющее условию

$$\dot{\bigcup_{x \in \mathcal{P}_0}} \Lambda_x = \mathbb{R}^n,$$

где $\dot{\bigcup}$ – символ объединения без пересечений, называется *фундаментальной областью решётки.* Множество $\mathcal{P}_0$ является фундаментальной областью решётки Λ, если

$$\mathcal{P}_\lambda \cap \mathcal{P}'_\lambda = \emptyset,\ \forall \lambda' \neq \lambda,\ \text{где } \mathcal{P}_\lambda = \mathcal{P}_0 + \lambda \text{ и } \bigcup_{\lambda \in \Lambda} \mathcal{P}_\lambda = \mathbb{R}^n.$$

Тогда любой вектор $x \in \mathbb{R}^n$ единственным образом может быть представлен в виде

$$x = \lambda + x_e,\ \lambda \in \Lambda,\ x_e \in \mathcal{P}_0,$$

где λ представляет собой результат квантования вектора x, обозначается как $\lambda = Q_{\mathcal{P}_0}(x)$, а

$$x_e = x \mathrm{mod}_{\mathcal{P}_0} \Lambda = x - Q_\Lambda(x)$$

называется ошибкой квантования. Можно определить квантайзер Вороного как

$$Q_{\mathcal{V}_\lambda}(x) = \arg\min_{\lambda\in\Lambda} \|x-\lambda\|, \tag{3.1}$$

где $\|\cdot\|$ – евклидова норма. Множество

$$\mathcal{V}_\lambda(\Lambda) = \{x : Q_\lambda(x) = \lambda \in \Lambda\}$$

называется ячейкой Вороного точки λ. Ячейка Вороного нулевой точки решётки $\mathcal{V}_0(\Lambda)$ является фундаментальной областью. В дальнейшем $x\mathrm{mod}_{\mathcal{P}_0}\Lambda$ будем обозначать как $x\mathrm{mod}\Lambda$ когда конкретная фундаментальная область не важна или ясна из контекста.

Утверждение 3.1 (Утв. 2.3.1 [76]). *Выполняется* $(x+\lambda)\mathrm{mod}\Lambda = x\mathrm{mod}\Lambda$, $\forall\lambda\in\Lambda$, *и* $(x\mathrm{mod}\Lambda + y)\mathrm{mod}\Lambda = (x+y)\mathrm{mod}\Lambda$.

Утверждение 3.2 (Утв. 2.2.1 [76]). *Объем решётки* $V(\Lambda)$, *определяющийся как объем фундаментальной области* $V(\mathcal{P}_0) = \int_{\mathcal{P}_0} dx$, *не зависит от выбора фундаментальной области и равен детерминанту решётки* $V(\Lambda) = \det(\Lambda)$.

Две решётки Λ_1 и Λ_2 называются вложенными $\Lambda_2 \subset \Lambda_1$, если базисные векторы решётки Λ_2 представляют собой целочисленные линейные комбинации базисных векторов решётки Λ_1. Другими словами, порождающие матрицы G_1 и G_2 решеток Λ_1 и Λ_2, соответственно, связаны соотношением $G_2 = G_1 J$, где J – $n\times n$ целочисленная матрица, детерминант которой не менее 1. Тогда

$$V(\Lambda_2) = \det(J)V(\Lambda_1).$$

Смежный класс решётки Λ_2 для некоторой точки $\lambda\in\Lambda_1$ определяется как

$$\Lambda_{2,\lambda} = \Lambda_2 + \lambda.$$

Множество всех смежных классов обозначается как

$$\Lambda_2/\Lambda_1 = \{\Lambda_{2,\lambda} : \lambda\in\Lambda_1\}.$$

Утверждение 3.3 (Утв. 8.2.1 [76]). *Количество различных смежных классов равно* $|\Lambda_2/\Lambda_1| = \frac{V(\Lambda_2)}{V(\Lambda_1)} = \det(J)$.

Пусть $\mathcal{P}_0(\Lambda_2)$ является некоторой фундаментальной областью решётки Λ_2. Множество $\Lambda_1 \cap \mathcal{P}_0(\Lambda_2)$ является фундаментальной областью решётки Λ_2 относительно решётки Λ_1. Тогда

$$\Lambda_1 = \dot{\bigcup_{\lambda\in\Lambda_1\cap\mathcal{P}_0(\Lambda_2)}} (\lambda+\Lambda_2),$$

причем $|\Lambda_1\cap\mathcal{P}_0(\Lambda_2)| = |\Lambda_2/\Lambda_1|$. Множество $\Lambda_1\cap\mathcal{P}_0(\Lambda_2)$ может быть выражено как

$$\Lambda_1\cap\mathcal{P}_0(\Lambda_2) = \Lambda_1\mathrm{mod}_{\mathcal{P}_0(\Lambda_2)}\Lambda_2.$$

Утверждение 3.4 (Утв. 8.2.2 [76]). *Каждая точка λ решётки Λ_1 единственным образом может быть выражена как $\lambda = \lambda_q + \lambda_e,\ \lambda_q \in \Lambda_2,\ \lambda_e \in \Lambda_1 \cap \mathcal{P}_0(\Lambda_2)$. А именно, точка λ_q решётки Λ_2 является единственной точкой такой, что $\lambda \in \lambda_q + \mathcal{P}_0(\Lambda_2)$, причем $\lambda_e = \lambda \mathrm{mod}_{\mathcal{P}_0(\Lambda_2)}\Lambda_2$.*

Следующее утверждение приведено в [76] без доказательства, поэтому докажем его.

Утверждение 3.5 (Утв. 8.4.2 [76]). *Для любых фундаментальных областей $\mathcal{P}_1 = \mathcal{P}_0(\Lambda_1)$ и $\mathcal{P}_2 = \mathcal{P}_0(\Lambda_2)$ вложенных решеток $\Lambda_2 \subset \Lambda_1$ выполняется*

(а) $\mathcal{P}_2 = \dot{\bigcup\limits_{\lambda \in \Lambda_1 \cap \mathcal{P}_2}} (\lambda + \mathcal{P}_1)$,

(б) $\mathcal{P}_2 = \dot{\bigcup\limits_{\lambda \in \Lambda_1 \cap \mathcal{P}_2}} ((\lambda + \mathcal{P}_1) \mathrm{mod}_{\mathcal{P}_2}\Lambda_2)$.

Доказательство. $\forall x \in \mathbb{R}^n$ можно единственным образом выразить как

$$x = \lambda_1 + x_{e_1},\ \lambda_1 \in \Lambda_1,\ x_{e_1} \in \mathcal{P}_1$$

и единственным образом как

$$x = \lambda_2 + x_{e_2},\ \lambda_2 \in \Lambda_2,\ x_{e_2} \in \mathcal{P}_2.$$

Так как $\Lambda_2 \subset \Lambda_1$, то согласно утверждению 3.4, λ_1 единственным образом выражается как

$$\lambda_1 = \tilde{\lambda}_2 + \lambda_e,\ \tilde{\lambda}_2 \in \Lambda_2,\ \lambda_e \in \Lambda_1 \cap \mathcal{P}_2.$$

Тогда $x = \tilde{\lambda}_2 + \lambda_e + x_{e_1}$. Но при заданной фундаментальной области единственной точкой Λ_2, которой равен квантайзер x является λ_2, следовательно, $\tilde{\lambda}_2 = \lambda_2$. Тогда

$$x = \lambda_2 + x_{e_2} = \lambda_2 + \lambda_e + x_{e_1} \Rightarrow x_{e_2} = \lambda_e + x_{e_1}.$$

Представление $x_{e_2} = \lambda_e + x_{e_1}$ единственно, что значит, что любая точка $x_{e2} \in \mathcal{P}_2$ принадлежит только одному из множеств $\{\lambda_e + \mathcal{P}_1 : \lambda_e \in \Lambda_1 \cap \mathcal{P}_2\}$. Тогда множества $\{\lambda_e + \mathcal{P}_1 : \lambda_e \in \Lambda_1 \cap \mathcal{P}_2\}$ не пересекаются. Для фиксированной λ_e $V(\lambda_e + \mathcal{P}_1) = V(\mathcal{P}_1) = V(\Lambda_1)$. Тогда

$$V(\dot{\bigcup_{\lambda_e \in \Lambda_1 \cap \mathcal{P}_2}} (\lambda_e + \mathcal{P}_1)) = |\Lambda_1 \cap \mathcal{P}_2| V(\Lambda_1) = \det(J) V(\Lambda_1).$$

Так как $V(\mathcal{P}_2) = \det(J)V(\Lambda_1)$, то

$$\mathcal{P}_2 = \dot{\bigcup_{\lambda_e \in \Lambda_1 \cap \mathcal{P}_2}} (\lambda_e + \mathcal{P}_1).$$

Равенство

$$\mathcal{P}_2 = \dot{\bigcup_{\lambda_e \in \Lambda_1 \cap \mathcal{P}_2}} ((\lambda_e + \mathcal{P}_1) \mathrm{mod}_{\mathcal{P}_2}\Lambda_2)$$

следует из того, что отображение $\mathrm{mod}_{\mathcal{P}_2}\Lambda_2 : \lambda_e + \mathcal{P}_1 \to \mathcal{P}_2,\ \forall \lambda_e \in \Lambda_1 \cap \mathcal{P}_2$ инъективно. ■

Докажем еще одно утверждение.

Утверждение 3.6. *Пусть* $\Lambda_2 \subset \Lambda_1$. $\forall x \in \mathbb{R}^n$ *выполняется* $Q_{\Lambda_1}(x \bmod \Lambda_2) = Q_{\Lambda_1}(x) \bmod \Lambda_2$ *и следовательно* $Q_{\Lambda_1}(x \bmod \Lambda_2) \bmod \Lambda_2 = Q_{\Lambda_1}(x) \bmod \Lambda_2$.

Доказательство. Для начала покажем что

$$Q_{\Lambda_1}(x - Q_{\Lambda_2}(x)) = Q_{\Lambda_1}(x) - Q_{\Lambda_2}(x).$$

Вектор x единственным образом выражается как

$$x = Q_{\Lambda_2}(x) + x_{\Lambda_2},\ Q_{\Lambda_2}(x) \in \Lambda_2,\ x_{\Lambda_2} \in \mathcal{P}_0(\Lambda_2).$$

В тоже время вектор x единственным образом может быть выражен как

$$x = Q_{\Lambda_1}(x) + x_{\Lambda_1},\ Q_{\Lambda_1}(x) \in \Lambda_1,\ x_{\Lambda_1} \in \mathcal{P}_0(\Lambda_1).$$

Тогда

$$x - Q_{\Lambda_2}(x) = \underbrace{Q_{\Lambda_1}(x) - Q_{\Lambda_2}(x)}_{\in \Lambda_1} + x_{\Lambda_1}$$

откуда следует что

$$Q_{\Lambda_1}(x - Q_{\Lambda_2}(x)) = Q_{\Lambda_1}(x) - Q_{\Lambda_2}(x).$$

Тогда

$$Q_{\Lambda_1}(x \bmod \Lambda_2) = Q_{\Lambda_1}(x_{\Lambda_2}) = Q_{\Lambda_1}(x - Q_{\Lambda_2}(x)) = Q_{\Lambda_1}(x) - Q_{\Lambda_2}(x).$$

Обозначим $Q_{\Lambda_1}(x) = \lambda_1$ и $Q_{\Lambda_2}(x) = \lambda_2$. Так как $\Lambda_2 \subset \Lambda_1$, то

$$\lambda_1 = \lambda_{1_2} + \lambda_{\Lambda_2},\ \lambda_{1_2} \in \Lambda_2,\ \lambda_{\Lambda_2} \in \Lambda_1 \cap \mathcal{P}_0(\Lambda_2).$$
$$x = \lambda_{1_2} + \lambda_{\Lambda_2} + x_{\Lambda_1}.$$

Согласно утверждению 3.5 $\lambda_{\Lambda_2} + x_{\Lambda_1} \in \mathcal{P}_0(\Lambda_2)$. По утверждению 3.4 для заданной фундаментальной области $\mathcal{P}_0(\Lambda_2)$ единственной точкой Λ_2, соответствующей x, является λ_2, следовательно, $\lambda_{1_2} = \lambda_2$. Тогда

$$Q_{\Lambda_1}(x \bmod \Lambda_2) = \lambda_1 - \lambda_2 = \lambda_{\Lambda_2} \in \Lambda_1 \cap \mathcal{P}_0(\Lambda_2).$$

В тоже время $Q_{\Lambda_1}(x) \bmod \Lambda_2 = \lambda_1 \bmod \Lambda_2 = \lambda_{\Lambda_2}$. ■

Теперь рассмотрим характеристики решёток, определяющие их применимость к кодированию источника и кодированию для канала. В первом случае будем говорить о решётках-квантователях (quantization good), а во втором – о AWGN успешных (AWGN good) решётках.

Задача квантования связана с задачей покрытия. Обозначим через $\Lambda + B_r$ множество сфер с центрами в точках решётки Λ радиуса r. Множество $\Lambda + B_r$ покрывает $\mathbb{R}^n$, если $\mathbb{R}^n \subseteq \Lambda + B_r$. Радиус покрытия решётки определяется как $r_{cov}(\Lambda) = \min\{r :\ \Lambda + B_r \text{ покрывает } \mathbb{R}^n\}$.

Определение 3.1. *Эффективным радиусом n-мерной решётки Λ называется радиус n-мерной сферы, объем которой равен объему решётки*

$$r_{eff}(\Lambda) = \left(\frac{V(\Lambda)}{V_n}\right)^{\frac{1}{n}},$$

где V_n – объем n-мерной сферы единичного радиуса, $V_n = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$.

Определение 3.2. *Покрывающая способность (covering efficiency) решётки определяется как*

$$\rho_{cov}(\Lambda) = \frac{r_{cov}(\Lambda)}{r_{eff}(\Lambda)}.$$

Говорят, что решётка обладает хорошей покрывающей способностью, если $\rho_{cov}(\Lambda)$ близко к 1. В этом случае, каждая точка пространства в среднем покрывается одной сферой.

Теорема 3.1 (Теорема 7.3.1 [76])**.** *Существует последовательность решеток Λ_n, такая что*

$$\rho_{cov}(\Lambda_n) \underset{n\to\infty}{\longrightarrow} 1,\ \log_2 \rho_{cov}(\Lambda_n) = O\left(\frac{\log_2 n}{n}\right).$$

Покрыть пространство $\mathbb{R}^n$ можно фундаментальными областями решётки. Говорят, что решётка хорошо выполняет операцию квантования, если средний квадрат ошибки квантования $Q(x) - x$ мал. Если в качестве фундаментальных областей выбрать ячейки Вороного, то $Q(x)$ задает квантайзер Вороного (3.1).

Определение 3.3. *Вторым моментом решётки Λ называется нормированный на размерность второй момент случайной величины U, равномерно распределенной в ячейке Вороного решётки $\mathcal{V}_0(\Lambda)$*

$$\sigma^2(\Lambda) = \frac{1}{V(\Lambda)}\frac{1}{n}\int\limits_{\mathcal{V}_0(\Lambda)} \|x\|^2 dx.$$

Характеристикой, определяющей способность решётки к квантованию, является *нормированный второй момент* (NSM).

Определение 3.4. *Нормированный второй момент определяется как*

$$G(\Lambda) = \frac{\sigma^2(\Lambda)}{V(\Lambda)^{\frac{2}{n}}}.$$

Для шара также можно определить NSM, причем шар обладает минимальным NSM среди всех фигур заданного объема.

Утверждение 3.7 (Следствие 7.2.1 [76])**.**

$$G(B_r) \underset{n\to\infty}{\longrightarrow} \frac{1}{2\pi e},\quad \log_2(2\pi e G(B_r)) = O\left(\frac{\log_2 n}{n}\right).$$

Теорема 3.2 (Теорема 7.1.2 [76]). *Для n-мерной решётки Λ, $n > 1$*

$$\rho_{cov}(\Lambda)^2 G(B_r) > G(\Lambda) > G(B_r).$$

По теореме 3.2, если решётка эффективна для покрытия, т.е. $\rho_{cov}(\Lambda) \to 1$, то она также является эффективной для квантования, т.е. $G(\Lambda)$ стремиться к минимальному значению $\frac{1}{2\pi e}$.

Теперь можно ввести определение решётки эффективной для квантования или *решётки-квантователя.*

Определение 3.5. *Последовательность решеток Λ_n называется решётками-квантователями, если*

$$G(\Lambda_n) \underset{n\to\infty}{\longrightarrow} \frac{1}{2\pi e}.$$

Известна эквивалентность между гауссовским распределением и равномерным распределением в шаре. Действительно, распределение белого гауссовского шума с нулевым средним зависит только от евклидовой нормы $\|z\|$, следовательно оно постоянно на сфере. По закону больших чисел $\frac{1}{n}\|z\|^2$ сходится по вероятности к дисперсии шума σ^2 при $n \to \infty$. Тогда распределение белого гауссовского шума с нулевым средним эквивалентно равномерному распределению по сфере радиуса $\sqrt{n\sigma^2}$. При $n \to \infty$ объем сферы приблизительно равен объему шара такого же радиуса. Следовательно, распределение белого гауссовского шума с нулевым средним эквивалентно равномерному распределению в шаре радиуса $\sqrt{n\sigma^2}$. Верно также и обратное, что равномерное распределение в шаре с увеличением размерности стремиться к гауссовскому распределению, в том смысле, что расстояния Кульбака-Лейблера между этими распределениями стремиться к 0 (теорема 7.2.3 [76]). Ячейка Вороного решётки-квантователя ведет себя как шар, в том смысле, что NSM решётки стремиться к NSM шара того же объема. Тогда равномерное распределение по ячейке Вороного решётки-квантователя стремиться к гауссовскому распределению.

Задача модуляции для AWGN канала связана с задачей упаковки. Вход AWGN канала X должен быть ограничен по мощности, то есть должен удовлетворять условию (3.8). Теорема о пропускной способности AWGN канала имеет геометрическую интерпретацию, связанную с упаковкой сфер. Зашумленный кодовый вектор длины n имеет нормальное распределение с математическим ожиданием равным значению кодового вектора и дисперсией равной дисперсии шума σ^2. С высокой вероятностью зашумленный вектор лежит внутри сферы радиуса $\sqrt{n\sigma^2}$. Таким образом, каждый кодовый вектор имеет в качестве области декодирования сферу радиуса $\sqrt{n\sigma^2}$. Для обеспечения малой вероятности ошибки декодирования эти сферы не должны пересекаться. В тоже время зашумленный вектор лежит внутри сферы радиуса $\sqrt{n(P+\sigma^2)}$. Следовательно, сферы радиуса $\sqrt{n\sigma^2}$ должны быть упакованы в сферу радиуса $\sqrt{n(P+\sigma^2)}$. Для достижения максимальной скорости передачи маленькие сферы должны быть упакованы

как можно плотнее. Декодирование по принципу максимального правдоподобия может быть выполнено с малой вероятностью ошибки.

Возьмем в качестве кодовых слов точки решётки Λ. Условие (3.8) для решётки в общем случае не выполняется, так как решётка не ограничена. Тогда понятие отношения сигнал/шум (SNR) теряет свой смысл. Вместо него вводят понятие *отношение объем/шум*.

Определение 3.6. *Отношение объем/шум (VNR) n-мерной решётки Λ при наличии AWGN шума с дисперсией σ^2 определяется как*

$$\mu(\Lambda, \sigma^2) = \frac{V(\Lambda)^{\frac{2}{n}}}{\sigma^2}.$$

В случае гауссовского шума распределение зашумленного вектора – это монотонная функция евклидовой нормы вектора. Тогда для решеток декодирование по принципу максимального правдоподобия сводится к нахождению квантайзера Вороного (3.1). В этом случае вероятность ошибки декодирования точки λ решётки Λ равна вероятности того, что зашумленный вектор Y лежит за пределами ячейки Вороного точки λ $P_{err} = P(Y \notin \mathcal{V}_\Lambda(\lambda))$ или, что вектор шума Z лежит за пределами ячейки Вороного решётки Λ, т.е. ячейки Вороного точки 0, т.е. $P_{err} = P(Z \notin \mathcal{V}(\Lambda))$. Тогда масштабируя решётку $\alpha\Lambda$, где α – это параметр, можно достигать заданного значения вероятности ошибки. Другими словами, можно подобрать решётку под заданное значение вероятности ошибки декодирования. Масштабирование решётки при фиксированном значении дисперсии шума эквивалентно масштабированию дисперсии шума при фиксированной решётке. Через $\sigma^2(\epsilon)$ обозначим такое значение σ^2, что $P_{err} = \epsilon$. Переопределим понятие VNR решётки, введя *нормированное отношение объем/шум*, которое характеризует решётку как код для AWGN канала

Определение 3.7. *Нормированное отношение объем/шум (NVNR) n-мерной решётки Λ при заданном значении вероятности ошибки P_{err} определяется как*

$$\mu(\Lambda, P_{err}) = \frac{V(\Lambda)^{\frac{2}{n}}}{\sigma^2(P_{err})}.$$

Для достижения наибольшей скорости передачи необходимо найти наиболее плотную решётку, т.е. решётку с наименьшим NVNR.

Теперь свяжем задачу выбора нужной решётки с задачей упаковки. Говорят, что множество $\Lambda + B_r$ есть упаковка пространства $\mathbb{R}^n$, если $\forall \lambda \neq \lambda'$ $(\lambda + B_r) \cap (\lambda' + B_r) = \emptyset$. *Радиус упаковки* решётки Λ определяется как $r_{pack}(\Lambda) = \sup\{r : \Lambda + B_r \text{ есть упаковка } \mathbb{R}^n\}$.

Определение 3.8. *Упаковочная способность (packing efficiency) решётки Λ определяется как*

$$\rho_{pack}(\Lambda) = \frac{r_{pack}(\Lambda)}{r_{eff}(\Lambda)}.$$

Для шара также можно определить NVNR, причем шар обладает минимальным NVNR среди всех фигур заданного объема.

Утверждение 3.8 (Следствие 7.2.1 [76])**.**

$$\mu(B_r, P_{err}) \underset{n\to\infty}{\longrightarrow} 2\pi e, \ \ \forall P_{err}\ 0 < P_{err} < 1.$$

Теорема 3.3 (Теорема 7.1.2 [76])**.** *Для n-мерной решётки Λ, $n > 1$*

$$\frac{1}{\rho_{pack}(\Lambda)^2}\mu(B_r, P_{err}) > \mu(\Lambda, P_{err}) > \mu(B_r, P_{err}).$$

По теореме 3.3, если решётка эффективна для упаковки, т.е. $\rho_{pack}(\Lambda) \to 1$, то она также является эффективной для модуляции, т.е. $\mu(\Lambda, P_{err})$ стремиться к минимальному значению $2\pi e$. Известно, что $\rho_{pack}(\Lambda)$ в пределе стремится к значению, которое строго меньше 1. Более того для каждого значения размерности $n \geq 1$ существует решётка, $\rho_{pack}(\Lambda)$ которой как минимум $\frac{1}{2}$ (следствие 7.6.1 [76]). Тем не менее, $\mu(\Lambda, P_{err})$ может достичь минимального значения $2\pi e$, если рассматривать упаковку с незначительным пересечением шаров [76]. Теперь можно определить *AWGN успешную решётку.*

Определение 3.9. *Последовательность решеток Λ_n называется AWGN успешной, если*

$$\mu(\Lambda_n, P_{err}) \underset{n\to\infty}{\longrightarrow} 2\pi e, \ \forall P_{err} : 0 < P_{err} < 1, \quad \log_2\left(\frac{\mu(\Lambda, P_{err})}{2\pi e}\right) = O\left(\frac{1}{\sqrt{n}}\right).$$

Ниже введем еще несколько понятий, которые понадобятся в дальнейшем. *Минимальное расстояние решётки* $d_{min}(\Lambda)$ определяется как

$$d_{min}(\Lambda) = \min_{\substack{\lambda,\lambda'\in\Lambda \\ \lambda\neq\lambda'}} \|\lambda - \lambda'\| = \min_{\lambda\in\Lambda, \lambda\neq 0} \|\lambda\|.$$

Шар $B_{r_{pack}(\Lambda)}$ с центром в точке 0 касается соседних шаров в одной точке. Центры касающихся шаров находятся на расстоянии $2r_{pack}(\Lambda)$, так как центры шаров – это точки решётки, то $d_{min}(\Lambda) = 2r_{pack}(\Lambda)$. Количество таких точек касания называется *контактным числом* (kissing number) N_Λ и определяется как количество точек, удаленных от точки 0 на минимальное расстояние $d_{min}(\Lambda)$

$$N_\Lambda = |\{\lambda \in \Lambda : \|\lambda\| = d_{min}(\Lambda)\}|.$$

Тэта-ряд решётки определяется как $\Theta_\Lambda(x) = \sum_{\lambda\in\Lambda} q^{\|\lambda\|^2}$, $q = e^{-\pi x}$, $x > 0$. Тэта-ряд так же можно представить в виде $\Theta_\Lambda(x) = \sum_{d\geq d_{min}(\Lambda)} N_\Lambda(d) q^{d^2}$, где $N_\Lambda(d)$ – количество точек решётки Λ с нормой d.

Для решётки Λ можно задать *двойственную* решётку $\Lambda^\star$.

Определение 3.10. *Решётка $\Lambda^\star$ называется двойственной к решётке Λ, если скалярное произведение её точек с точками Λ есть целое число, то есть $< \lambda^\star, \lambda > \in \mathbb{Z}$, $\forall \lambda \in \Lambda$, $\lambda^\star \in \Lambda^\star$.*

Иными словами базис решётки $\Lambda^\star$ формируют строки матрицы $\mathbf{G}^{-1}$, где $\mathbf{G}$ – порождающая матрица решётки Λ. Тогда порождающая матрица $\Lambda^\star$ определяется как $(\mathbf{G}^{-1})^\top$, следовательно, детерминант $\Lambda^\star$ связан с детерминантом Λ выражением

$$V(\Lambda^\star) = \det(\Lambda^\star) = \det((\mathbf{G}^{-1})^\top) = \frac{1}{\det(\mathbf{G})} = \frac{1}{V(\Lambda)}. \tag{3.2}$$

Определение 3.11. *Функция $f : \mathbb{R}^n \to \mathbb{R}$ называется Λ-периодической, если $f(x + \lambda) = f(x)$, $\forall \lambda \in \Lambda$.*

Для функции $f : \mathcal{P}_0(\Lambda) \to \mathbb{R}$ можно задать преобразование Фурье

$$f(x) = \sum_{\lambda^\star \in \Lambda^\star} \hat{f}(\lambda^\star) e^{2\pi i < x, \lambda^\star >}, \tag{3.3}$$

где

$$\hat{f}(\lambda^\star) = \frac{1}{V(\Lambda)} \int_{\mathcal{P}_0(\Lambda)} f(x) e^{-2\pi i < x, \lambda^\star >} dx.$$

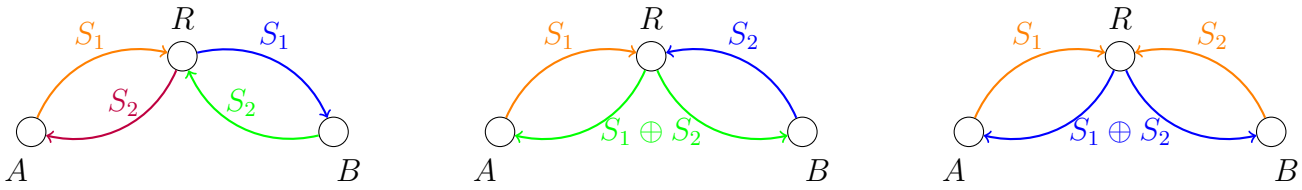
Если f – Λ-периодическая, то (3.3) верно для любого $x \in \mathbb{R}^n$.

Лемма 3.1 (Формула Пуассона)**.**

$$f(\Lambda) = \sum_{\lambda \in \Lambda} f(\lambda) = V(\Lambda^\star) \sum_{\lambda^\star \in \Lambda^\star} \hat{f}(\lambda^\star) = V(\Lambda^\star) \hat{f}(\Lambda^\star).$$

3.1.2 Введение в аналоговое сетевое кодирование

Рассмотрим пример, иллюстрирующий идею физического сетевого кодирования (рис. 3.1). Два источника A и B обмениваются сообщениями S_1 и S_2 с помощью промежуточного узла R. При традиционном способе передачи (рис. 3.1а) для этого понадобится четыре временных слота. Передача в различных временных слотах представлена на рисунке стрелками различных цветов. В первом временном слоте узел A передает свое сообщение узлу R. В следующем временном слоте узел R передает это сообщение узлу B. Аналогичным образом в течение следующих двух временных слотах сообщение узла B будет передано узлу A. Рисунок 3.1б иллюстрирует использование цифрового сетевого кодирования. В первых двух временных слотах узлы A и B по очереди передают свои сообщения узлу R. В третьем слоте узел R передает сумму полученных сообщений, из которой узлы A и B могут восстановить необходимую информацию. Промежуточный узел R может сразу получать такую сумму, если узлы A и B будут передавать свои сообщения в одном слоте. В этом и состоит идея сетевого кодирования на физическом уровне. В этом случае для обмена сообщениями понадобятся только два слота (рис. 3.1в).



(а) Традиционный способ передачи

(б) Сетевое кодирование

(в) Сетевое кодирование на физическом уровне

Рис. 3.1: Иллюстрация различных способов передачи для беспроводной сети

Было предложено несколько схем передачи, которые можно отнести к физическому сетевому кодированию. Одна из наиболее удачных и широко исследуемых Compute-and-Forward (CF) предложена в [77].

Для реализации сетевого кодирования на физическом уровне необходимо подобрать код, который бы удовлетворял нескольким требованиям. Во-первых, он должен быть эффективен, то есть достигать пропускной способности AWGN канала. Во-вторых, он должен обладать линейной структурой, чтобы наложение сигналов, которое происходит на физическом уровне, имело бы своим результатом кодовое слово. Основная идея сетевого кодирования состоит в том, чтобы передавать по сети линейные комбинации сообщений, которые есть элементы конечного поля. Последнее требование к коду заключается в том, чтобы линейные комбинации кодовых слов можно было бы отображать в линейные комбинации над конечным полем. Это гарантирует, что принятая сумма сигналов представляет собой на самом деле сумму сообщений. Всем этим требованиям отвечают коды на решётках.

В самом общем виде идею метода [77] можно описать следующим образом. Источники кодируют свои сообщения, принадлежащие некоторому полю, в точки решётки. Промежуточные узлы получают сообщения, представляющие собой зашумленные линейные комбинации точек решётки, и восстанавливают из принятых сообщений целочисленные линейные комбинации точек решётки, которые передают далее. Получатели линейные комбинации точек решётки отображают в линейные комбинации сообщений из поля. При условии, что к получателям приходит достаточное количество линейных комбинаций, они могут восстановить интересующие их сообщения. Предполагается, что промежуточные узлы знают коэффициенты передачи каналов, соединяющих их с отправителями. Выигрыш в скорости передачи, по сравнению с традиционными методами, достигается за счет того, что промежуточные узлы декодируют линейные комбинации сообщений, а не отдельные сообщения, рассматривая остальные как шум. Более того, промежуточные узлы могут определять какие именно линейные комбинации восстанавливать. Наибольших скоростей можно достичь, если восстанавливать линейные комбинации с коэффициентами близкими к коэффициентам передачи.

Пусть выбраны вложенные решётки $\Lambda_2 \subset \Lambda_1$, заданные на $\mathbb{R}^n$. Эти решётки определяют код C_{Λ_1,Λ_2}, кодовые слова которого составляют множество $\Lambda_1 \cap \mathcal{V}(\Lambda_2)$. Источники кодируют свои сообщения $m_l \in \mathbb{F}_p^k$, где p – простое, а $l \in \{1, 2, \ldots, L\}$–порядковый номер источника, в кодовые слова $x_l \in \mathbb{R}^n$, $\|x_l\|^2 \leq nP$. Некоторый i-й промежуточный узел получает

$$y_i = \sum_{l=1}^{L} h_{i,l} x_l + z_i,$$

где $h_i = (h_{i,1}, h_{i,2}, \ldots, h_{i,L}) \in \mathbb{R}^L$ – коэффициенты передачи, а z_i – гауссовский шум $z_i \sim N(0, \mathbf{I}_n)$. Промежуточный узел пытается восстановить линейную комбинацию точек решётки с вектором коэффициентов $a_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,L}) \in \mathbb{Z}^L$

$$v_i = (\sum_{l=1}^{L} a_{i,l} t_l) \mathrm{mod} \Lambda_2,$$

где $t_l \in \Lambda_1 \cap \mathcal{V}(\Lambda_2)$ и модуль берется по ячейке Вороного $\mathcal{V}(\Lambda_2)$. Полученный вектор v_i затем можно будет преобразовать в линейную комбинацию исходных сообщений

$$u_i = \bigoplus_{l=1}^{L} q_{i,l} m_l,$$

где $\bigoplus$ обозначает сложение в поле $\mathbb{F}_p$ и $q_{i,l} \in \mathbb{F}_p$. Выбор вектора коэффициентов a_i определяется двумя факторами. Первый состоит в том, чтобы максимизировать скорость передачи

$$R(h_i, a_i) = \frac{1}{2} \log_2^+ \left(\left(\|a_i\|^2 - \frac{P(h_i a_i^\top)^2}{1 + P\|h_i\|^2} \right)^{-1} \right),$$

где $\log_2^+ x = \max(\log_2 x, 0)$. Второй фактор заключается в том, что вектор a_i выбирается так, чтобы промежуточный узел мог восстановить необходимую комбинацию сообщений m_l, $l \in \{1, 2, \ldots, L\}$. Между коэффициентами $q_{i,j}$ и $a_{i,j}$ можно установить соответствие

$$q_{i,j} = g^{-1}(a_{i,j} \mathrm{mod} p),$$

где $g^{-1} : \{0, 1, \ldots, p-1\} \to \mathbb{F}_p$. Если бы $a_{i,l} = h_{i,l}$, то в качестве x_l можно было бы просто брать точки t_l, но $h_{i,l} \neq a_{i,l}$. Выразим y_i в виде

$$y_i = \sum_{l=1}^{L} a_{i,l} x_l + \sum_{l=1}^{L} (h_{i,l} - a_{i,l}) x_l + z.$$

Слагаемые $(h_{i,l} - a_{i,l})x_l$ действуют как дополнительный шум. Этот дополнительный шум необходимо, во-первых, уменьшить, а во-вторых, сделать независимым от соответствующего информационного вектора t_l, так как зависимость шума от исходного вектора влечет за собой нежелательные эффекты при квантовании. Независимость достигается с помощью дизеринга, суть которого определяет следующая лемма.

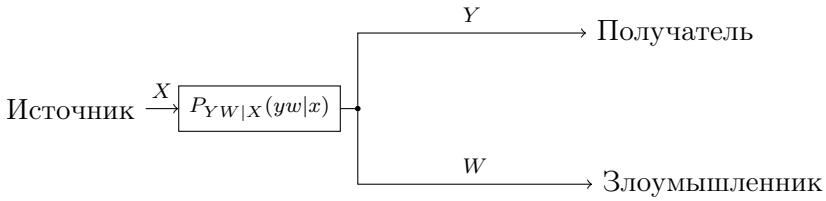


Рис. 3.2: Канал с подслушиванием типа I

Лемма 3.2 (Лемма 4.1.1 [76]). *Пусть заданы решётка* Λ *и вектор* s*, имеющий некоторое распределение на* $\mathbb{R}^n$*. Если вектор* v *равномерно распределен в фундаментальной области* $\mathcal{P}_0$ *решётки* Λ*, то вектор* $(s-v)\mathrm{mod}_{\mathcal{P}_0}\Lambda$ *равномерно распределен в* $\mathcal{P}_0$ *и не зависит от* s*.*

Каждый отправитель имеет дизер d_l, известный всем узлам. Кодовое слово x_l есть искаженная дизером точка кода C_{Λ_1,Λ_2}, соответствующая сообщению m_l, то есть

$$x_l = (t_l - d_l)\mathrm{mod}\Lambda_2.$$

Для уменьшения шума коэффициенты $h_{i,l}$ должны быть как можно ближе к желаемым $a_{i,l}$. Это достигается за счет фильтрации Винера, которая уменьшает среднеквадратичную ошибку между вектором v_i и его оценкой $\hat{v}_i$ и заключается в масштабировании принятого вектора y_i параметром $\alpha_i = \frac{Ph_i^\top a_i}{1+P\|h_i\|^2}$. Получив y_i, промежуточный узел оценит v_i как

$$\hat{v}_i = (Q_{\Lambda_1}(\alpha_i y_i + \sum_{l=1}^{L} a_{i,l}d_l))\mathrm{mod}\Lambda_2.$$

При наличии нужного количества линейных комбинаций u_i получатели могут восстановить необходимые им сообщения $m_l,\ l \in \{1,2,\ldots,L\}$. Достаточные условия для восстановления сообщений даны в [77].

3.2 Канал с подслушиванием типа I

Вайнер [1] рассматривал передачу сообщения секретно по каналу с отводом. Этот канал в литературе часто называют каналом с подслушиванием типа I. Канал представлен на рисунке 3.2. В общем виде канал с подслушиванием задается матрицей переходных вероятностей $P_{YW|X}(yw|x)$. Канал с отводом можно представить как два дискретных канала без памяти: основной и отводный. Основной – это канал между источником и получателем с входным алфавитом $\mathbb{X}$, выходным алфавитом $\mathbb{Y}$ и матрицей переходных вероятностей $P_{Y|X}(y|x)$, а отводный – канал между источником и злоумышленником с входным алфавитом $\mathbb{X}$, выходным алфавитом $\mathbb{W}$ и матрицей переходных вероятностей $P_{W|X}(w|x)$. Вайнер рассматривал физически ухудшенный канал, для которого выполняется $P_{YW|X}(yw|x) = P_{Y|X}(y|x)P_{W|Y}(w|y)$. В этом

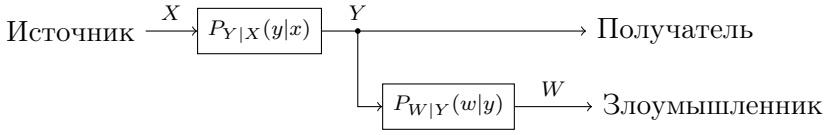


Рис. 3.3: Ухудшенный канал с подслушиванием типа I

случае отводный канал есть стохастически ухудшенная версия основного канала $P_{W|X}(w|x) = \sum_{y\in\mathbb{Y}} P_{W|Y}(w|y)P_{Y|X}(y|x)$ (рис. 3.3), где вход каналов X, выход основного канала Y и выход канала злоумышленника W образуют цепь Маркова $X \to Y \to W$. В работе [1] исходные сообщения M рассматриваются как случайные величины равномерно распределенные на множестве сообщений $\mathbb{M}$, $|\mathbb{M}| = 2^{nR}$. В качестве критерия секретности Вайнер рассматривал условие слабой секретности (1.4). Получателю сообщение M должно быть передано надежно, то есть необходим детерминированный декодер $g : \mathbb{Y} \to \mathbb{M}$ с вероятностью ошибки

$$P(g(Y) \neq M) \leq \epsilon \; \forall \epsilon > 0. \tag{3.4}$$

При рассмотрении канала с подслушиванием первоочередной является задача определения *секретной пропускной способности*. Под секретной пропускной способностью понимается максимальное количество символов, которое может быть передано секретно при условии, что сообщение безошибочно может быть восстановлено получателем. Модель канала является жизнеспособной, если его секретная пропускная способность больше нуля. Секретная пропускная способность C_s определяется как максимум значения скорости R, для которой (3.4) и (1.4) выполняются для любого $\epsilon > 0$ и достаточно большого n. В работе [1] показано, что

$$R \leq C_s = \max_{X\to Y\to W}(I(X;Y) - I(X;W)). \tag{3.5}$$

Для достижения этой секретной пропускной способности Вайнер предложил идею, суть которой состоит в том, чтобы не использовать всю пропускную способность основного канала для передачи информации, а резервировать часть пропускной способности для передачи случайных символов, которые призваны запутать злоумышленника. Эта идея предъявляет требование к конструкции кода. Код C должен состоять из множества подкодов $\{C_1, C_2, \dots C_{|\mathbb{M}|}\}$. Источник каждому сообщению M ставит в соответствие C_M, $M = 1, 2 \dots |\mathbb{M}|$ и передает случайно выбранное из C_M кодовое слово $X \in \mathbb{X}$. Информативной частью сообщения X является индекс подкода, которому оно принадлежит. Идея Вайнера реализуется, если мощность подкодов не менее $2^{nI(X;W)}$. Это приводит к тому, что вся пропускная способность канала злоумышленника расходуется на случайные символы.

Секретная пропускная способность канала с подслушиванием общего вида определяется как [3]

$$C_s = \max_{U\to X\to(Y,W)}(I(U;Y) - I(U;W)), \tag{3.6}$$

для случайных величин, составляющих цепь Маркова $U \to X \to (Y, W)$.

В работе [4] было предложены две другие модели отводного канала. Первую модель назовем медленным отводным каналом. В этом случае отводной канал имеет меньшую пропускную способность, чем основной $I(X;Y) \geq I(X;W)$ для всех распределений X. Вторую модель назовем шумным отводным каналом. Для него выполняется $I(V;Y) \geq I(V;W)$ для всех цепей Маркова $V \to X \to (Y, W)$. Секретная пропускная способность при медленном отводном канале и шумном отводном канале задается выражениями (3.5) и (3.6) соответственно. Медленный отводной канал – наиболее слабая модель из трех возможных моделей отводного канала. Рассмотрим пример, представленный в работе [78].

$$\mathbb{X} = \{1,2,3\},\ \mathbb{Y} = \mathbb{W} = \{1,2\},\ P_{Y|X}(y|x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix},\ P_{W|X}(w|x) = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Из этих данных следует, что $I(X;Y) \geq I(X;W)$ для любого распределения X. Но для

$$U = f(X) = \begin{cases} 0, \text{ при } X = 1 \text{ или } X = 2, \\ 1, \text{ при } X = 3, \end{cases}$$

и $P(X=1) = P(X=2) = \frac{1}{4},\ P(X=3) = \frac{1}{2}$ имеем $I(U;Y) = 0$ и $I(U;W) > 0$. Таким образом, отводный канал является медленным, но не является шумным. Ухудшенный канал представляет собой наиболее сильную модель. В работе [4] показана следующая взаимосвязь между моделями

$$\text{ухудшенный канал } \to \text{ шумный канал } \to \text{ медленный канал.}$$

В работе [5] показано, что C_s (3.6) может быть достигнута при условии строгой секретности (1.3). С точки зрения теории кодирования условия слабой и сильной секретности можно интерпретировать следующим образом. При увеличении длины кодового слова средняя вероятность ошибки декодирования на стороне злоумышленника стремится к единице. Эти два критерия секретности отличаются скоростью схождения вероятности ошибки к единице. При условии строгой секретности вероятность ошибки сходится экспоненциально [6]. При слабой секретности со скоростью $o(1)$, что нетрудно показать. Перепишем условие слабой секретности в виде

$$\frac{1}{n} I(M;W) \leq \tau_n, \text{ где } \lim_{n\to\infty} \tau_n = 0, \text{ то есть } \tau = o(1).$$

Воспользуемся леммой Фано

Лемма 3.3 (Лемма 7.3 [69]). *Пусть $\hat{M}$– оценка M и $p_e = P(\hat{M} \neq M)$– вероятность ошибочного решения. Тогда*

$$H(M|\hat{M}) \leq h(p_e) + p_e \log_2(|\mathbb{M}| - 1),$$

где $h(p_e) = -p_e \log_2(p_e) - (1-p_e)\log_2(1-p_e)$.

Так как $H(M|\hat{M}) \geq H(M|W)$ и $\max\limits_{p_e} h(p_e) = 1$, то $1 + p_e \log_2(|\mathbb{M}| - 1) \geq H(M|W)$. Тогда

$$p_e \geq \frac{H(M|W) - 1}{\log_2(|\mathbb{M}| - 1)} \geq \frac{H(M|W) - 1}{\log_2 |\mathbb{M}|} \geq \frac{H(M) - n\tau_n}{\log_2 |\mathbb{M}|} = \frac{\log_2 |\mathbb{M}| - n\tau_n}{\log_2 |\mathbb{M}|} = 1 - \frac{n\tau_n}{\log_2 2^{nR}} = 1 - \frac{\tau_n}{R}.$$

Откуда следует, что p_e сходится к 1 со скоростью $o(1)$.

В криптографии на практике не используется модели, предполагающие, что сообщение – это случайная величина. В криптографии используют понятие *семантической секретности*, которое формулируется для конкретных сообщений. Для канала с подслушиванием семантическую секретность определяют следующим образом.

Определение 3.12 ([10]). *Сообщение M семантически секретно, если*

$$\lim_{n\to\infty} \sup_{f,M} (2^{-H_\infty(f(M)|W)} - 2^{-H_\infty(f(M))}) = 0,$$

где $H_\infty(M) = -\log_2(\max\limits_m P(M = m))$ и супремум берется по всем случайным величинам M, заданным на $\mathbb{M}$ и всем функциям f на множестве $\mathbb{M}$.

Неформально семантическую секретность можно описать так: имея W, злоумышленник не может оценить значение некоторой функции f от сообщения M лучше, чем если бы он просто угадывал $f(M)$ без знания W. Семантическая секретность не предполагает простого условия на взаимную информацию. В работах [10, 11] было показано, что строгая секретность для всех распределений исходного сообщения для канала с подслушиванием типа I эквивалентна семантической секретности. Это позволяет сформулировать для семантической секретности условие на взаимную информацию. Семантическая секретность достигается, если

$$\exists \gamma > 0, n_0 : \ \forall n > n_0 \ \max_{P(M)} I(M; W) \leq e^{-n\gamma}, \tag{3.7}$$

где максимум берется по всем распределениям исходного сообщения M.

В работе [7] рассматривается гауссовский канал с подслушиванием, где отводный канал есть ухудшенная версия основного (рис. 3.4). Сообщение M источника кодируется в слово X длины n. Выход основного канала Y и отводного канала W имеют вид

$$\begin{cases} Y = X + U_1, \\ W = X + U_2. \end{cases}$$

Вектор шума U_1 не зависит от вектора шума U_2. Компоненты векторов U_1 и U_2 – независимые одинаково распределенные случайные величины с распределением $N(0, \sigma_1^2)$ и $N(0, \sigma_2^2)$ соответственно. Вход канала должен быть ограничен по мощности

$$\frac{1}{n} E(\|X^2\|) \leq P. \tag{3.8}$$

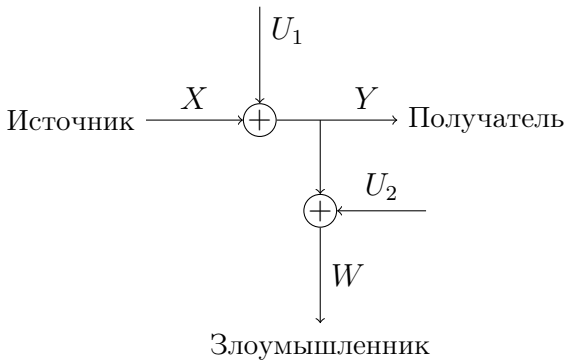


Рис. 3.4: Гауссовский канал с подслушиванием типа I

Секретная пропускная способность такого канала выражается как

$$C_s = \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_1^2}\right) - \log_2\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right).$$

Известно, что для дискретного канала с подслушиванием наиболее криптостойким является код с максимальным расстоянием. Совершенной секретности можно достичь, если злоумышленник прослушивает не более чем $d'-1$ символов сообщения, где d'– расстояние двойственного кода. Следовательно, код с максимальным расстоянием обеспечивает совершенную секретность для наиболее сильного злоумышленника, так как d' в этом случае максимально. Для гауссовского канала с подслушиванием также вводят критерий криптостойкости используемого кода. Авторы работы [79] предложили понятие *криптостойкой* решётки.

Определение 3.13. *Пусть на $\mathbb{R}^n$ заданы распределения P_X и Q_X. Статистическим расстоянием между этими распределениями называется $\Delta(P_X, Q_X) = \int\limits_{\mathbb{R}^n} |P_X(x) - Q_X(x)|dx$. Если распределения P_X и Q_X дискретные и заданы на множестве A, то $\Delta(P_X, Q_X) = \sum\limits_{x\in A} |P_X(x) - Q_X(x)|$.*

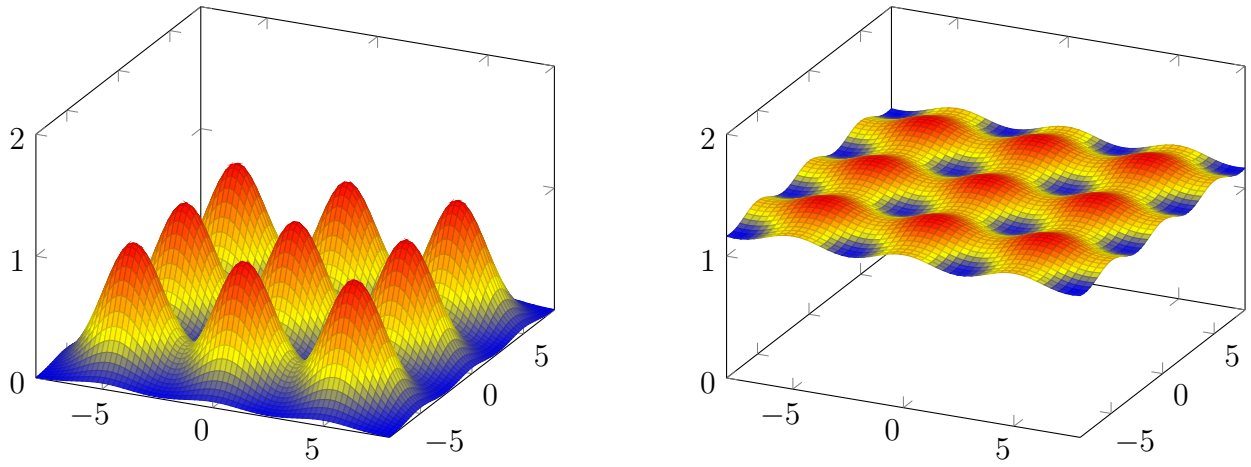
В работе [79] предложен способ кодирования для гауссовского канала с подслушиванием, отвечающий условию секретности (3.7). Секретность доказывается с помощью техники предложенной в [5], суть которой состоит в следующем. Можно показать, что выход канала злоумышленника $\mathcal{W}$ «почти» не зависит от исходного сообщения M, где «почти» понимается как малость среднего статистического расстояния

$$d = \sum_{m\in\mathbb{M}} P_M(m)\Delta(P_{\mathcal{W}|M=m}, P_{\mathcal{W}}),$$

где $\mathbb{M}$ – множество сообщений.

Лемма 3.4 (Лемма 1 [5, 79])**.** *Для $|\mathbb{M}| \geq 4$*

$$\frac{1}{2}d^2 \leq I(M;\mathcal{W}) \leq d\log_2\frac{|\mathbb{M}|}{d}.$$



(а) $\sigma^2 = 1.5$ (б) $\sigma^2 = 5$

Рис. 3.5: $f_{\sigma,\Lambda}$ для $\Lambda = 5\mathbb{Z}^2$ и разных значений σ^2

Верхняя граница для d определяется леммой 2 из [5]. Приведем здесь эту лемму в том виде, в котором она дана в работе [79].

Лемма 3.5 (Лемма 2 [5, 79]). *Для любого распределения $Q_{\mathcal{W}}$, заданного на $\mathbb{R}^n$, справедливо*

$$d \leq 2 \sum_{m \in \mathbb{M}} P_M(m) \Delta(P_{\mathcal{W}|M=m}, Q_{\mathcal{W}}).$$

Верхняя граница для d определяется параметрами решётки, а именно *уровнем плато* (flatness factor) решётки, понятие которого вводят авторы статьи [79].

Гауссовское распределение на $\mathbb{R}^n$ с дисперсией σ^2 и математическим ожиданием $c \in \mathbb{R}^n$ задаётся плотностью распределения

$$f_{\sigma,c}(x) = \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\frac{\|x-c\|^2}{2\sigma^2}}.$$

Для заданной решётки Λ можно определить Λ-периодическое гауссовское распределение как

$$f_{\sigma,\Lambda}(x) = \sum_{\lambda \in \Lambda} f_{\sigma,\lambda}(x) = \frac{1}{(\sqrt{2\pi}\sigma)^n} \sum_{\lambda \in \Lambda} e^{-\frac{\|x-\lambda\|^2}{2\sigma^2}}. \tag{3.9}$$

Определение 3.14. *Уровень плато для решётки Λ и параметра σ определяется как*

$$\epsilon_\Lambda(\sigma) = \max_{x \in \mathcal{P}(\Lambda)} \left| \frac{f_{\sigma,\Lambda}(x)}{\frac{1}{V(\Lambda)}} - 1 \right|.$$

Уровень плато определяет максимальное отклонение распределения $f_{\sigma,\Lambda}(x)$ на некоторой фундаментальной области решётки $\mathcal{P}(\Lambda)$ от равномерного распределения на этой фундаментальной области. Уровень плато также является характеристикой решётки при декодировании

по максимальному правдоподобию [80]. Рассмотрим рисунок 3.5. При большом значении уровня плато (рис. 3.5а) гауссовские колоколы хорошо разделимы, что обеспечивает верное декодирование. При маленьком значении (рис. 3.5б) в верхней части гауссовских колоколов образуется плато, гауссовское распределение становится похоже на равномерное. Это приводит к неоднозначности при декодировании, но в тоже время может быть использовано для обеспечения секретности, так как становится сложно отличить два разных колокола. Уровень плато монотонно убывает с увеличением σ, $\epsilon_\Lambda(\sigma_2) \leq \epsilon_\lambda(\sigma_1)$ при $\sigma_1 < \sigma_2$.

Утверждение 3.9 (Утверждение 2 [79])**.**

$$\epsilon_\Lambda(\sigma) = \left(\frac{\mu(\Lambda, \sigma^2)}{2\pi}\right)^{\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1.$$

Тогда уровень плато будет большим при высоком значении VNR и маленьким при маленьком VNR. Основной результат для ограничения среднего статистического расстояния d с помощью уровня плато сформулирован в следующем утверждении.

Утверждение 3.10 (Утверждение 4 [79])**.** *Пусть $\bar{f}(\cdot)$ есть плотность вероятности величины $x \mathrm{mod}_{\mathcal{P}(\Lambda)}\Lambda$, где x имеет плотность распределения $f_{\sigma,c}$ для некоторого $c \in \mathbb{R}^n$, а $U_{\mathcal{P}(\Lambda)}$ задаёт плотность равномерного распределения на $\mathcal{P}(\Lambda)$. Тогда*

$$\Delta(\bar{f}, U_{\mathcal{P}(\Lambda)}) \leq \epsilon_\Lambda(\sigma).$$

Для выполнения условия секретности (3.7) необходимо, чтобы уровень плато решётки Λ экспоненциально убывал.

Определение 3.15. *Последовательность решёток Λ_n называется криптостойкой, если*

$$\epsilon_{\Lambda^{(n)}} = e^{-\Omega(n)} \ \ \forall \mu(\Lambda_n, \sigma) < 2\pi.$$

3.3 Частный случай канала: modΛ канал

3.3.1 Модель сети

Сеть представляется направленным графом $G(V, E)$, вершины V которого есть узлы сети, а ребра E – беспроводные соединения. Соединение представляет собой modΛ гауссовский канал, представленный на рисунке 3.6. Сообщения передаются по принципу физического сетевого кодирования. В сети присутствуют L источников сообщений и N получателей. В общем случае $L \neq N$. Между источниками и получателями может осуществляться как одноадресная передача, так и многоадресная, когда сообщение некоторого источника должно быть передано некоторому подмножеству получателей.

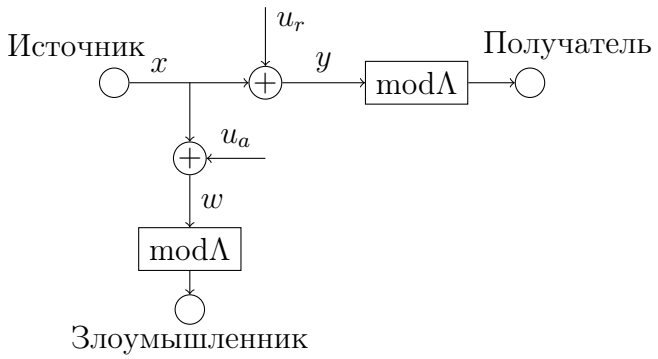


Рис. 3.6: modΛ канал с подслушиванием типа I

3.3.2 Кодирование источника

Источники предварительно кодируют свои сообщения по схеме секретной передачи, предложенной в [79]. Пусть в $\mathbb{R}^n$ заданы n-мерные решётки $\Lambda_s \subset \Lambda_a \subset \Lambda_r$, такие что

$$\frac{1}{n}\log_2|\Lambda_r/\Lambda_a| = R,\ \frac{1}{n}\log_2|\Lambda_a/\Lambda_s| = R'.$$

Решётка Λ_a выбирается так, чтобы она являлась решёткой-квантователем, а для выполнения условия (3.8) необходимо $\sigma^2(\Lambda_s) = P$. Решётка Λ_r должна быть AWGN успешной, а решётка Λ_a криптостойкой.

Источник устанавливает взаимно однозначное соответствие между множеством сообщений $\mathbb{M} = \{1, \ldots, 2^{nR}\}$ и множеством смежных классов Λ_r/Λ_a, то есть каждому $m \in \mathbb{M}$ ставится в соответствие $\lambda_m \in \Lambda_r \cap \mathcal{P}_0(\Lambda_a)$. Затем равномерно выбирается точка $\lambda \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s)$, и источник отправляет $\mathcal{X} = \lambda_m + \lambda$. Точка $\mathcal{X}$ принадлежит смежному классу $\Lambda_a + \lambda_m$ и равномерно распределена в этом смежном классе. Сообщения $\mathcal{Y}$ получателя и $\mathcal{W}$ злоумышленника выражаются как

$$\begin{cases} \mathcal{Y} = (\mathcal{X} + \mathcal{U}_r)\text{mod}\Lambda_s, \\ \mathcal{W} = (\mathcal{X} + \mathcal{U}_a)\text{mod}\Lambda_s, \end{cases} \tag{3.10}$$

где $\mathcal{U}_r, \mathcal{U}_a$ – n-мерные векторы, имеющие распределения $f_{\sigma_r,0}, f_{\sigma_a,0}$, соответственно. Тогда отношение сигнал/шум на стороне получателя определяется как $\text{SNR}_r = \frac{P}{\sigma_r^2}$, а на стороне злоумышленника $\text{SNR}_a = \frac{P}{\sigma_a^2}$.

В [79] показано, что $\Delta(P_{\mathcal{W}|M=m}, U_{\mathcal{V}_0(\Lambda_s)}) \leq \epsilon_{\Lambda_a}(\sigma_a)$. Тогда по лемме 3.5 $d \leq 2\epsilon_{\Lambda_a}(\sigma_a)$ и по лемме 3.4

$$I(M;\mathcal{W}) \leq 2\epsilon_{\Lambda_a}(\sigma_a)(nR - \log_2(2\epsilon_{\Lambda_a}(\sigma_a)),$$

причем это неравенство выполнено для произвольного распределения M. Так как Λ_a – криптостойкая решётка, то есть $\epsilon_{\Lambda_a}(\sigma_a)$ экспоненциально убывает, то $I(M;\mathcal{W})$ экспоненциально убывает, откуда следует, что M передаётся семантически секретно.

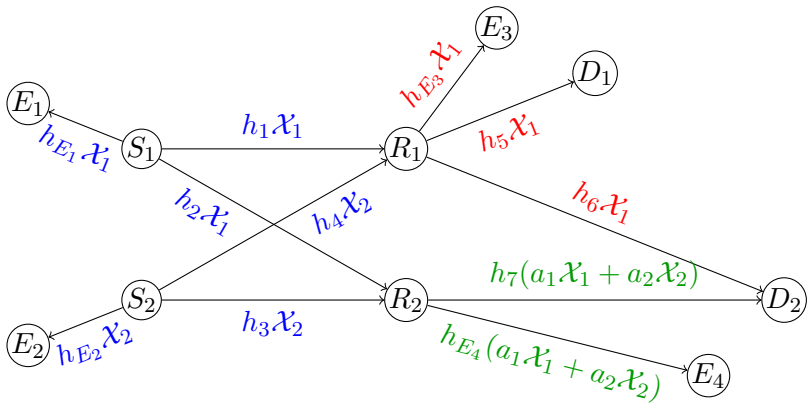


Рис. 3.7: Пример работы сети

Этот результат согласуется со следующей идеей обеспечения секретности для канала с подслушиванием. Для того чтобы передать сообщение секретно нужно передавать со скоростью большей пропускной способности канала злоумышленника. Более того, желательно, чтобы злоумышленник не мог декодировать ничего кроме случайных символов. Следовательно, скорость передачи случайных символов должна превосходить пропускную способность канала злоумышленника. Пропускная способность канала злоумышленника

$$C(\Lambda_s, \sigma_a^2) = \frac{1}{n}(\log_2 V(\Lambda_s) - h(\Lambda_s, \sigma_a^2)),$$

где $h(\Lambda_s, \sigma_a^2)$ – дифференциальная энтропия шума $\mathcal{U}_a \mathrm{mod} \Lambda_s$. Так как Λ_s – это решётка-квантователь, то, во-первых, распределение $\mathcal{U}_a \mathrm{mod} \Lambda_s$ близко к распределению белого гауссовского шума, то есть $h(\Lambda_s, \sigma_a^2) = \frac{1}{2}\log_2 2\pi e\sigma_a^2$, а, во-вторых, $V(\Lambda_s) \to 2\pi e\sigma(\Lambda_s) = 2\pi eP$. Тогда

$$C(\Lambda_s, \sigma_a^2) = \frac{1}{2}(\log_2 2\pi eP - \log_2 2\pi e\sigma_a^2) = \frac{1}{2}\log_2 \mathrm{SNR}_a.$$

Случайные символы задаются равномерно распределённой точкой $\lambda \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s)$. Скорость передачи случайных символов равна $R' = \frac{1}{n}\log_2 |\Lambda_a/\Lambda_s|$. Выразим её через SNR_a.

$$\mu(\Lambda_a, \sigma_a) = \frac{V(\Lambda_a)^{\frac{2}{n}}}{\sigma_a^2} \overset{(1)}{=} \frac{V(\Lambda_s)^{\frac{2}{n}}}{2^{nR'\frac{2}{n}}\sigma_a^2} \overset{(2)}{\to} \frac{2\pi eP}{2^{nR'}\sigma_a^2} < 2\pi,$$

где (1) следует из того, что $\Lambda_s \subset \Lambda_a$, следовательно, $|\Lambda_s/\Lambda_a| = \frac{V(\Lambda_s)}{V(\Lambda_a)} = 2^{nR'} \Rightarrow V(\Lambda_a) = \frac{V(\Lambda_s)}{2^{nR'}}$, а (2) следует из того, что Λ_s – решётка-квантователь. Тогда $R' > \frac{1}{2}\log_2 \mathrm{SNR}_a + \frac{1}{2}$ и выполняется $R' > C(\Lambda_s, \sigma_a^2)$.

3.3.3 Модель злоумышленника

Рассматривается внешний пассивный глобальный адаптивный злоумышленник, канал которого есть $\mathrm{mod}\Lambda$ гауссовский канал. Канал злоумышленника зашумлен больше, чем прослушиваемый им канал между легальными узлами сети.

Выясним какую информацию злоумышленник может выделить из перехваченных сообщений. Вероятность верного декодирования точки λ_m решётки Λ_r равна вероятности того, что зашумленный вектор $\mathcal{W}$ (3.16) лежит внутри ячейки Вороного точки λ_m. Вероятность того, что злоумышленник верно декодирует точку решётки Λ_r можно оценить сверху как ([81])

$$P \leq \frac{1}{(\sqrt{2\pi}\sigma_a)^n} V(\Lambda_r) \sum_{t \in \Lambda_a} e^{-\frac{\|t\|^2}{2\sigma_a^2}} = \frac{1}{(\sqrt{2\pi}\sigma_a)^n} V(\Lambda_r) \Theta_{\Lambda_a}\left(\frac{1}{2\pi\sigma_a^2}\right). \tag{3.11}$$

Так как решётка Λ_a криптостойкая, то уровень плато этой решётки мал и согласно утверждению (3.9), значение тэта-ряда решётки в точке $\frac{1}{2\pi\sigma_a^2}$ мало. Следовательно, вероятность верного декодирования мала. При этом злоумышленник может с малой вероятностью ошибки декодировать точки решётки Λ_a. Покажем это.

$$\begin{aligned} P_{err} &= P(Q_{\Lambda_a}(\mathcal{W}) \neq \lambda) \overset{\text{Утв. } 3.6}{=} P(Q_{\Lambda_a}(\lambda + \lambda_m + \mathcal{U}_a) \bmod \Lambda_s \neq \lambda) \\ &= P(\lambda_m + \mathcal{U}_a \notin \mathcal{V}_0(\Lambda_a)) = P(\lambda_m + \mathcal{U}_a \text{ ближе к некоторой } \lambda' \in \Lambda_a,\ \lambda' \neq 0,\ \text{чем к } 0). \end{aligned} \tag{3.12}$$

Зафиксируем λ_m, тогда $\lambda_m + \mathcal{U}_a$ имеет распределение f_{σ_a, λ_m}. Вероятность ошибки (3.12) можно оценить сверху как сумму вероятностей $P(\lambda_m + \mathcal{U}_a$ ближе к $\lambda' \in \Lambda_a,\ \lambda' \neq 0,$ чем к $0)$ для всех таких λ'.

Утверждение 3.11 (Утверждение 13.5.1 [76])**.**

$$P(\lambda_m + \mathcal{U}_a \textit{ ближе к } \lambda' \in \Lambda_a,\ \lambda' \neq 0,\ \textit{чем к } 0) = F\left(\frac{\|\lambda'\|}{2\sigma_a}\right),$$

где $F(x) = \int\limits_x^\infty f_z dz$, f_z *– нормальное распределение.*

Так как точки λ' отличные от 0, могут находится от 0 на расстоянии не менее, чем $d_{min}(\Lambda_a)$, то

$$P_{err} \leq \sum_{d \geq d_{min}} N_{\Lambda_a}(d) F\left(\frac{d}{2\sigma_a}\right). \tag{3.13}$$

Так как $F(x) \leq \frac{1}{2} e^{-\frac{x^2}{2}}$, то

$$P_{err} \leq \sum_{d \geq d_{min}} N_{\Lambda_a}(d) e^{-\frac{d^2}{8\sigma_a^2}}.$$

Оценим тэта-ряд как

$$\Theta_{\Lambda_a}\left(\frac{1}{2\pi\sigma_a^2}\right) = \sum_{t \in \Lambda_a} e^{-\frac{\|t\|^2}{2\sigma_a^2}} \simeq 1 + \sum_{\substack{t \in \Lambda_a, \\ \|t\| = d_{min}(\Lambda_a)}} e^{-\frac{\|t\|^2}{2\sigma_a^2}} = 1 + N_{\Lambda_a} e^{-\frac{d_{min}^2}{2\sigma_a^2}}.$$

Как уже было сказано, для того чтобы минимизировать вероятность (3.11), нужно минимизировать $\Theta_{\Lambda_a}(\frac{1}{2\pi\sigma_a^2})$. Для достаточно большого d_{min} ($d_{min}^2/\sigma_a^2 \gg 1$) наибольший вклад в сумме (3.13) вносит первое слагаемое, тогда

$$P_{err} \leq N_{\Lambda_a} e^{-\frac{d_{min}^2}{8\sigma_a^2}}.$$

Для достаточно большого d_{min} выполняется $N_{\Lambda_a} e^{-\frac{d_{min}^2}{8\sigma_a^2}} < 1 + N_{\Lambda_a} e^{-\frac{d_{min}^2}{2\sigma_a^2}}$. Тогда

$$P_{err} \leq \Theta_{\Lambda_a}\left(\frac{1}{2\pi\sigma_a^2}\right).$$

Следовательно, минимизируя вероятность (3.11), то есть делая решётку Λ_a криптостойкой, мы в тоже время минимизируем вероятность (3.12). Это значит, что злоумышленник может декодировать точки решётки Λ_a с приемлемой вероятностью ошибки.

В схеме семантически секретной передачи точки решётки Λ_a задают «случайность» внутри смежного класса. Покажем на примере как злоумышленник может использовать свою способность декодировать «случайность». Обратимся к примеру на рисунке 3.7. В сети имеется два источника S_1, S_2 и два получателя D_1 и D_2. Источник S_1 передаёт сообщение m_1 узлам D_1, D_2, а источник S_2 передаёт сообщение m_2 узлу D_2. По сети от S_1 к D_1, D_2 передаётся $\mathcal{X}_1 = \lambda_{m_1} + \lambda_1$, а от S_2 к D_2 передаётся $\mathcal{X}_2 = \lambda_{m_2} + \lambda_2$, где $\lambda_{m_1}, \lambda_{m_2}$ задают смежные классы, определяемые сообщениями m_1 и m_2 соответственно, а λ_1, λ_2 выбираются случайно равномерно из $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$. Различные цвета на рисунке 3.7 обозначают различные временные слоты, в которых передаются сообщения. Коэффициенты $h_{(\cdot)}$ являются коэффициентами передачи соответствующих каналов. Для того чтобы вычислить пары источник-отправитель, злоумышленник может расставить своих агентов E_1, E_2, E_3, E_4 как показано на рисунке. В одном и том же временном слоте E_1 получает сообщение $\mathcal{W}_{E_1} = (h_{E_1}\mathcal{X}_1 + \mathcal{U}_{E_1}) \mathrm{mod} \Lambda_s$, а E_2 – сообщение $\mathcal{W}_{E_2} = (h_{E_2}\mathcal{X}_2 + \mathcal{U}_{E_2}) \mathrm{mod} \Lambda_s$. Из полученного сообщения E_1 может извлечь λ_1, а E_2 – λ_2. Это даёт возможность злоумышленнику заключить, что источник S_1 отправил сообщение со «случайностью» λ_1, а источник S_2 сообщение со «случайностью» λ_2. В следующем временном слоте E_3 получает $\mathcal{W}_{E_3} = (h_{E_3}\mathcal{X}_1 + \mathcal{U}_{E_3}) \mathrm{mod} \Lambda_s$. Результатом декодирования этого сообщения является точка λ_1, из чего злоумышленник может сделать вывод, что узел D_1 – это адресат сообщения источника S_1. В третьем временном слоте E_4 примет сообщение $\mathcal{W}_{E_4} = (h_{E_4}(a_1\mathcal{X}_1 + a_2\mathcal{X}_2) + \mathcal{U}_{E_4}) \mathrm{mod} \Lambda_s$, декодируя которое можно получить линейную комбинацию $a_3\lambda_1 + a_4\lambda_2 = \hat{\lambda} \in \Lambda_a$. Так как злоумышленнику известны λ_1 и λ_2, а также коэффициенты a_3, a_4, то проверив, что $\hat{\lambda} \neq a_3\lambda_1$, $\hat{\lambda} \neq a_4\lambda_1$, $\hat{\lambda} \neq a_3\lambda_2$, $\hat{\lambda} \neq a_4\lambda_2$, $\hat{\lambda} \neq a_3\lambda_2 + a_4\lambda_1$ и наконец $\hat{\lambda} = a_3\lambda_1 + a_4\lambda_2$, он может заключить, что D_2 получает сообщения как от S_1, так и от S_2.

В общем случае, когда сеть значительно сложнее, чем представленная на рисунке 3.7, на месте получателей D_1, D_2 могут быть промежуточные узлы R_3, R_4, которые будут передавать сообщения далее. Тогда описанным выше способом злоумышленник способен прослеживать сообщения вдоль их маршрута. В общем случае i-й агент злоумышленника получает сообщение $\mathcal{W}_{E_i} = (\sum\limits_j h_{E_i,j}\mathcal{X}_j + \mathcal{U}_{E_i}) \mathrm{mod} \Lambda_s$, которое декодируется в линейную комбинацию $\sum\limits_j a_{E_i,j}\lambda_j$, где коэффициенты $a_{E_i,j}$ определяются злоумышленником. Следовательно, злоумышленник имеет возможность находить соответствие между сообщениями, определяя, как описано выше, какие известные ему «случайности» формируют конкретную линейную комбинацию «случайностей».

3.3.4 Совершенная несвязываемость

Промежуточные узлы должны обеспечить несвязываемость входящих и выходящих сообщений и в большей степени несвязываемость случайных частей сообщений. Пусть $\mathcal{X}^{in} = \lambda_m + \lambda_1$. Точка $\mathcal{X}^{in}$ принадлежит смежному классу $\Lambda_a + \lambda_m$. Рассмотрим точку

$$\mathcal{X}^{out} = (\mathcal{X}^{in} + \lambda_2)\mathrm{mod}\Lambda_s = (\lambda_m + \lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s \overset{\text{Утв. 3.1}}{=} (\lambda_m + (\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s)\mathrm{mod}\Lambda_s,$$

где λ_2 выбирается равномерно на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и независимо от $\mathcal{X}^{in}$. Так как $\lambda_1 + \lambda_2 \in \Lambda_a$, то $(\lambda_1+\lambda_2)\mathrm{mod}\Lambda_s \in \Lambda_a \cap \mathcal{V}(\Lambda_s)$ и $\mathcal{X}^{out} \in \Lambda_a + \lambda_m$. Точка $\mathcal{X}^{out}$ принадлежит тому же смежному классу, что и $\mathcal{X}^{in}$, значит переносит ту же информацию. Так как $\lambda_m \in \mathcal{P}_0(\Lambda_a)$, тогда по утверждению 3.5 $\lambda_m+(\lambda_1+\lambda_2)\mathrm{mod}\Lambda_s \in \mathcal{V}_0(\Lambda_s)$ и, следовательно, $(\lambda_m+(\lambda_1+\lambda_2)\mathrm{mod}\Lambda_s)\mathrm{mod}\Lambda_s = \lambda_m+(\lambda_1+\lambda_2)\mathrm{mod}\Lambda_s$, т.е.

$$\mathcal{X}^{out} = \lambda_m + (\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s.$$

Обозначим случайную часть сообщения $\mathcal{X}^{out}$ через $\hat{\lambda}$, т.е. $(\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s = \hat{\lambda}$.

Лемма 3.6. *Пусть точка λ_2 равномерно распределена на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$. Тогда точка $\hat{\lambda} = (\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s$ равномерна на $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и не зависит от λ_1.*

Доказательство. $\lambda_1+\lambda_2 = Q_{\Lambda_s}(\lambda_1+\lambda_2)+\hat{\lambda} \Rightarrow \lambda_2 = Q_{\Lambda_s}(\lambda_1+\lambda_2)+\hat{\lambda}-\lambda_1$. Так как $\lambda_2 \in \Lambda_a \cap \mathcal{V}_0(\Lambda_s)$, то $\lambda_2 = \lambda_2\mathrm{mod}\Lambda_s = (\hat{\lambda} - \lambda_1)\mathrm{mod}\Lambda_s$. Тогда $P_{\hat{\lambda}|\lambda_1}(\tilde{\lambda}, \tilde{\lambda}_1) = P_{\lambda_2}((\tilde{\lambda} - \tilde{\lambda}_1)\mathrm{mod}\Lambda_s) = \frac{1}{2^{nR'}}$ для любого значения λ_1. ■

Следовательно, случайные части сообщений $\mathcal{X}^{in}$ и $\mathcal{X}^{out}$ независимы. Заметим, что лемма 3.6 устраняет необходимость использования дополнительного дизера в схеме кодирования источника.

Теорема 3.4. *При заданной точке λ_m точка $\mathcal{X}^{out}$ имеет равномерное распределение и не зависит от $\mathcal{X}^{in}$.*

Доказательство. Покажем что, $H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_m) = H(\mathcal{X}^{out}|\lambda_m) = H((\lambda_1 + \lambda_2)\mathrm{mod}\Lambda_s) = H(\hat{\lambda})$. Так как $\hat{\lambda}$ равномерна на $\Lambda_a \cap \mathcal{V}(\Lambda_s)$, то $H(\hat{\lambda}) = \log_2 |\Lambda_a \cap \mathcal{V}(\Lambda_s)| = nR'$.

$$\begin{aligned} H(\mathcal{X}^{out}\mathcal{X}^{in}\lambda_1\lambda_2|\lambda_m) &= H(\lambda_1|\lambda_m) + H(\lambda_2|\lambda_1\lambda_m) + H(\mathcal{X}^{in}|\lambda_1\lambda_2\lambda_m) \\ &\quad + H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_1\lambda_2\lambda_m) \\ &= H(\mathcal{X}^{in}|\lambda_m) + H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_m) + H(\lambda_1|\mathcal{X}^{out}\mathcal{X}^{in}\lambda_m) \\ &\quad + H(\lambda_2|\mathcal{X}^{out}\mathcal{X}^{in}\lambda_1\lambda_m). \end{aligned} \tag{3.14}$$

$$
\begin{aligned}
&H(\lambda_1|\lambda_m) = H(\lambda_1) = nR',\\
&H(\lambda_2|\lambda_1\lambda_m) = H(\lambda_2) = nR',\\
&H(\mathcal{X}^{in}|\lambda_1\lambda_2\lambda_m) = H(\mathcal{X}^{in}|\lambda_1\lambda_m) = 0, \text{ так как } \mathcal{X}^{in} = \lambda_1 + \lambda_m,\\
&H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_1\lambda_2\lambda_m) \le H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_2) = 0, \text{ так как } \mathcal{X}^{out} = (\mathcal{X}^{in} + \lambda_2)\mathrm{mod}\Lambda_s,\\
&H(\mathcal{X}^{in}|\lambda_m) = H(\lambda_1) = nR',\\
&H(\lambda_1|\mathcal{X}^{out}\mathcal{X}^{in}\lambda_m) = 0,\\
&H(\lambda_2|\mathcal{X}^{out}\mathcal{X}^{in}\lambda_1\lambda_m) \le H(\lambda_2|\mathcal{X}^{out}\mathcal{X}^{in}).
\end{aligned}
\tag{3.15}
$$

$\mathcal{X}^{out} = (\mathcal{X}^{in} + \lambda_2)\mathrm{mod}\Lambda_s \Rightarrow \mathcal{X}^{in} + \lambda_2 = Q_{\Lambda_s}(\mathcal{X}^{in} + \lambda_2) + \mathcal{X}^{out} \Rightarrow \lambda_2 = Q_{\Lambda_s}(\mathcal{X}^{in} + \lambda_2) + \mathcal{X}^{out} - \mathcal{X}^{in}$. Так как $\lambda_2 \in \mathcal{V}(\Lambda_s)$, то $\lambda_2\mathrm{mod}\Lambda_s = \lambda_2$. Тогда $\lambda_2 = (Q_{\Lambda_s}(\mathcal{X}^{in} + \lambda_2) + \mathcal{X}^{out} - \mathcal{X}^{in})\mathrm{mod}\Lambda_s \overset{\text{Утв. 3.1}}{=} (\mathcal{X}^{out} - \mathcal{X}^{in})\mathrm{mod}\Lambda_s$. Следовательно, $H(\lambda_2|\mathcal{X}^{out}\mathcal{X}^{in}) = 0$. Из (3.14) и (3.15) следует, что

$$H(\mathcal{X}^{out}|\mathcal{X}^{in}\lambda_m) = nR'.$$

■

Из теоремы 3.4 следует

$$I(\mathcal{X}^{out}; \mathcal{X}^{in}|\lambda_m) = 0.$$

Рассмотрим i-й промежуточный узел, который в общем случае принимает сообщение

$$\mathcal{Y}_i^{in} = (\sum_j h_{ij}\mathcal{X}_j^{in} + \mathcal{U}_{r_i})\mathrm{mod}\Lambda_s.$$

Узел декодирует это сообщение с коэффициентами $\{a_{ij}\}$, $j = 1, \ldots, L$, где L – количество входных каналов узла, другими словами, количество соседей узла, от которых он может принимать сообщения. В результате

$$\mathcal{X}_i^{in} = Q_{\Lambda_r}(\mathcal{Y}_i^{in})\mathrm{mod}\Lambda_s \overset{\text{Утв. 3.6}}{=} (\sum_j a_{ij}\mathcal{X}_j^{in})\mathrm{mod}\Lambda_s,$$

выбирает λ_2 случайно и равномерно из $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и формирует сообщение для дальнейшей передачи

$$
\begin{aligned}
\mathcal{X}_i^{out} = (\mathcal{X}_i^{in} + \sum_j a_{ij}\lambda_2)\mathrm{mod}\Lambda_s &= ((\sum_j a_{ij}\mathcal{X}_j^{in})\mathrm{mod}\Lambda_s + \sum_j a_{ij}\lambda_2)\mathrm{mod}\Lambda_s\\
&\overset{\text{Утв. 3.1}}{=} (\sum_j a_{ij}\mathcal{X}_j^{in} + \sum_j a_{ij}\lambda_2)\mathrm{mod}\Lambda_s = (\sum_j a_{ij}\mathcal{X}_j^{out})\mathrm{mod}\Lambda_s,
\end{aligned}
$$

Обозначим $a_i = \sum_j a_{ij}$. Так как коэффициенты a_{ij} целочисленны, то $a_i\lambda_2 \in \Lambda_a$. Точка $(a_i\lambda_2)\mathrm{mod}\Lambda_s$ равномерно распределена в $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$. Так как

$$\mathcal{X}_i^{out} = (\mathcal{X}_i^{in} + a_i\lambda_2)\mathrm{mod}\Lambda_s = (\mathcal{X}_i^{in} + (a_i\lambda_2)\mathrm{mod}\Lambda_s)\mathrm{mod}\Lambda_s,$$

то по лемме 3.6

$$I(\mathcal{X}_i^{out}; \mathcal{X}_i^{in}) = 0.$$

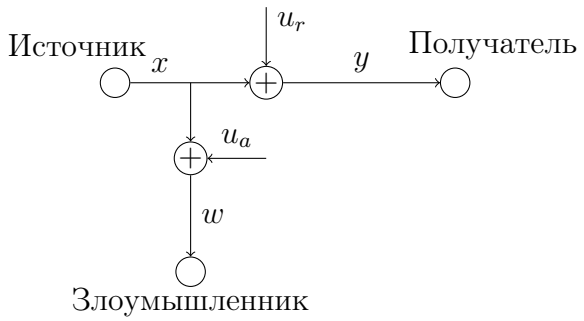


Рис. 3.8: Гауссовский канал с подслушиванием типа I

3.4 Канал общего вида

Теперь рассмотрим метод несвязываемости для общего случая. В качестве модели злоумышленника примем модель, представленную в разделе 3.3.3.

3.4.1 Кодирование источника

Метод семантически секретной передачи по гауссовскому каналу с подслушиванием общего вида (рис. 3.8) также представлен в [79]. Сообщения $\mathcal{Y}$ получателя и $\mathcal{W}$ злоумышленника выражаются как

$$\begin{cases} \mathcal{Y} = \mathcal{X} + \mathcal{U}_r, \\ \mathcal{W} = \mathcal{X} + \mathcal{U}_a, \end{cases} \tag{3.16}$$

где $\mathcal{U}_r, \mathcal{U}_a$ – n-мерные векторы, имеющие распределения $f_{\sigma_r,0}, f_{\sigma_a,0}$, соответственно.

Рассматриваются две заданные на $\mathbb{R}^n$ вложенные решётки $\Lambda_a \subset \Lambda_r$ такие, что $\frac{1}{n}\log_2|\Lambda_r/\Lambda_a| = R$. Источник устанавливает взаимно однозначное соответствие между множеством сообщений $\mathbb{M} = \{1, \ldots, 2^{nR}\}$ и множеством смежных классов Λ_r/Λ_a, то есть каждому $m \in \mathbb{M}$ ставится в соответствие $\lambda_m \in \Lambda_r \cap \mathcal{P}_0(\Lambda_a)$. Случайную часть сообщения предлагается выбирать согласно *дискретному гауссовскому* распределению, заданному на решётке Λ_r.

Дискретное гауссовское распределение на решётке Λ с центром в $\mu \in \mathbb{R}^n$ задаётся функцией

$$D_{\Lambda,\sigma,\mu}(\lambda) = \frac{f_{\sigma,\mu}(\lambda)}{f_{\sigma,\Lambda}(\mu)},\ \forall \lambda \in \Lambda,$$

где $f_{\sigma,\Lambda}(\mu)$ – периодическое распределение (3.9). Это распределение также может быть задано на смежном классе

$$D_{\Lambda-\mu,\sigma,0}(\lambda-\mu) = \frac{f_{\sigma,0}(\lambda-\mu)}{f_{\sigma,\Lambda}(\mu)},\ \forall \lambda \in \Lambda,$$

причем $D_{\Lambda,\sigma,\mu}(\lambda) = D_{\Lambda-\mu,\sigma,0}(\lambda-\mu)$.

Определение 3.16. *Для решётки* Λ *и* $\epsilon > 0$ *коэффициентом сглаживания (smoothing parameter)* $\eta_\epsilon(\Lambda)$ *называется минимальное* σ *такое, что* $\sum_{\lambda^\star \in \Lambda^\star \setminus \{0\}} e^{-2\pi\sigma^2\|\lambda^\star\|^2} \leq \epsilon$.

Между коэффициентом сглаживания и уровнем плато есть чёткая связь.

Утверждение 3.12 (Утверждение 3 [79])**.** *Если* $\sigma = \eta_\epsilon(\Lambda)$*, то* $\epsilon_\Lambda(\sigma) = \epsilon$.

Коэффициент сглаживания определяет значение дисперсии, при которой дискретное гауссовское распределение ведет себя как непрерывное. Это поведение выражается в следующей лемме.

Лемма 3.7 (Лемма 8, [79], Утверждение 3.9 [82])**.** *Пусть* g *есть распределение случайной величины, заданной как сумма двух величин, одна из которых имеет непрерывное гауссовское распределение* $f_{\sigma,0}$*, а другая – дискретное гауссовское распределение* $D_{\Lambda-\mu,\sigma_0,0}$*, то есть*

$$g(x) = \frac{1}{f_{\sigma,\Lambda}(\mu)} \sum_{t \in \Lambda - \mu} f_{\sigma_0,0}(t) f_{\sigma,0}(x-t).$$

$g(x)$ *задано на* $\mathbb{R}^n$*. Если* $\epsilon = \epsilon_\Lambda(\frac{\sigma_0\sigma}{\sqrt{\sigma_0^2+\sigma^2}}) < \frac{1}{2}$*, то*

$$\Delta(g, f_{\sqrt{\sigma_0^2+\sigma^2},0}) \leq 4\epsilon.$$

Лемма 3.7 утверждает, что при достаточно большом коэффициенте сглаживания (или достаточно маленьком уровне плато) сумма дискретной гауссовской величины и непрерывной гауссовской величины представляет собой «почти» сумму двух непрерывных гауссовских величин.

В методе, предложенном в [79], случайная часть сообщения λ выбирается согласно распределению $D_{\Lambda_a,\sigma_s,-\lambda_m}$. Тогда итоговое сообщение $\mathcal{X} = \lambda_m + \lambda$ распределено на смежном классе $\Lambda_a + \lambda_m$ по закону $D_{\Lambda_a+\lambda_m,\sigma_s,0}$, где σ_s выбирается так, чтобы сообщения, передаваемые в канал, удовлетворяли ограничению по мощности (3.8), то есть $\sigma_s^2 = P$.

Обозначим $\tilde{\sigma_e} = \frac{\sigma_e\sigma_s}{\sqrt{\sigma_e^2+\sigma_s^2}}$, а через $\epsilon_{\Lambda_a}(\tilde{\sigma_e})$ обозначим уровень плато решётки Λ_a с параметром $\tilde{\sigma_e}$.

Тогда, если $\epsilon_{\Lambda_a}(\tilde{\sigma_e}) < \frac{1}{2}$, то $\Delta(P_{\mathcal{W}|M=m}, f_{\sqrt{\sigma_e^2+\sigma_s^2},0}) \leq 4\epsilon_{\Lambda_a}(\tilde{\sigma_e})$. По леммам 3.5 и 3.4

$$I(M;\mathcal{W}) \leq 8\epsilon_{\Lambda_a}(\tilde{\sigma_e})(nR - \log_2 8\epsilon_{\Lambda_a}(\epsilon(\tilde{\sigma_e}))).$$

Последнее неравенство говорит о том, что сообщение M передаётся семантически секретно, если решётка Λ_a криптостойкая.

Лемма 3.7 определяет важное с практической точки зрения преимущество этого метода, заключающееся в том, что нет необходимости использовать дизер. Декодирование происходит по правилу

$$\hat{\lambda}_m = Q_{\Lambda_r}(\alpha\mathcal{Y}) \mathrm{mod} \Lambda_a, \tag{3.17}$$

где $\alpha =$ – коэффициент Винера, о котором говорилось в пункте 3.2.2.

$$\hat{\lambda}_m = Q_{\Lambda_r}(\mathcal{X} + (\alpha-1)\mathcal{X} + \alpha\mathcal{U}_r)\mathrm{mod}\Lambda_a \overset{\text{Утв. } 3.6}{=} Q_{\Lambda_r}((\lambda_m + \lambda + (\alpha-1)\mathcal{X} + \alpha\mathcal{U}_r)\mathrm{mod}\Lambda_a)\mathrm{mod}\Lambda_a$$
$$= Q_{\Lambda_r}(\lambda_m + (\alpha-1)\mathcal{X} + \alpha\mathcal{U}_r)\mathrm{mod}\Lambda_a.$$

Величина $\tilde{\mathcal{U}} = (\alpha-1)\mathcal{X} + \alpha\mathcal{U}_r$ представляет собой эквивалентный шум. Величина $\alpha\mathcal{U}_r$ распределена как $f_{\alpha\sigma_r,0}$, а $(\alpha-1)\mathcal{X}$ как $D_{(\alpha-1)(\Lambda_a+\lambda_m),(\alpha-1)\sigma_s,0}$. По лемме 3.7 при заданном значении сообщения m распределение эквивалентного шума близко к независящему от m гауссовскому распределению $f_{\tilde{\sigma}_r,0}$, где $\tilde{\sigma}_r = \sqrt{(\alpha-1)^2\sigma_s^2 + \alpha^2\sigma_r^2}$. Таким образом, шум $\tilde{\mathcal{U}}$ не зависит от λ_m, и дизер при кодировании использовать не нужно.

3.4.2 Модель сети

Рассматривается модель сети аналогичная модели, представленной в пункте 3.3.1 за исключением того, что соединения представляют собой гауссовский канал с подслушиванием общего вида (рис. 3.8).

В работе [83] говорится о возможности использовать метод семантической секретности [79], представленный в предыдущем пункте, для такой сети, но не даётся строгих обоснований этой возможности. Для обоснования того, что метод [79] можно с канала распространить на сеть, которая работает по принципу сетевого кодирования на физическом уровне, обеспечивая при этом тот же уровень секретности и надежности передачи, необходимо показать, что сумма точек решётки, имеющих дискретное гауссовское распределение, также имеет дискретное гауссовское распределение. Выполнение этого условия позволяет также сохранить преимущество метода [79], состоящее в том, что дизер при кодировании использовать не нужно.

Теорема 3.5. *Пусть $\mathcal{X}_1$ имеет распределение $D_{\Lambda,\sigma_1,\mu_1}$, а $\mathcal{X}_2$ распределение $D_{\Lambda,\sigma_2,\mu_2}$, и пусть $\epsilon_\Lambda(\frac{\sigma_1\sigma_2}{\sqrt{\sigma_1^2+\sigma_2^2}}) = \epsilon < \frac{1}{6}$. Рассмотрим $\mathcal{Y} = \mathcal{X}_1 + \mathcal{X}_2$. Статистическое расстояние между распределением величины $\mathcal{Y}$ и распределением $D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}$ не превосходит 12ϵ.*

Доказательство. Воспользуемся техникой доказательства утверждения 3.9 [82].

$$P_{\mathcal{Y}}(y) = \frac{1}{f_{\sigma_1,\Lambda}(\mu_1)}\frac{1}{f_{\sigma_2,\Lambda}(\mu_2)}\sum_{t\in\Lambda} f_{\sigma_1,\mu_1}(t) f_{\sigma_2,\mu_2}(y-t)$$
$$= \frac{1}{(\sqrt{2\pi}\sigma_1)^n(\sqrt{2\pi\sigma_2})^n}\frac{1}{f_{\sigma_1,\Lambda}(\mu_1)}\frac{1}{f_{\sigma_2,\Lambda}(\mu_2)}\sum_{t\in\Lambda} e^{-\frac{\|t-\mu_1\|^2}{2\sigma_1^2}+\frac{\|y-t-\mu_2\|}{2\sigma_2^2}}. \qquad (\star)$$

Воспользовавшись определением евклидовой нормы $\|x\| = \sqrt{\sum_i x_i^2}$, можно привести

$\frac{\|t-\mu_1\|^2}{2\sigma_1^2} + \frac{\|y-t-\mu_2\|^2}{2\sigma_2^2}$ к виду $\frac{\|y-(\mu_1+\mu_2)\|^2}{2(\sigma_1^2+\sigma_2^2)} + \frac{\sigma_1^2+\sigma_2^2}{2\sigma_1^2\sigma_2^2}\|t - \frac{\sigma_1^2}{\sigma_1^2+\sigma_2^2}(y + (\frac{\sigma_2^2}{\sigma_1^2}\mu_1 - \mu_2))\|^2$.

$$(\star) = \frac{e^{-\frac{\|y-(\mu_1+\mu_2)\|^2}{2(\sigma_1^2+\sigma_2^2)}}}{(\sqrt{2\pi}\sigma_1)^n(\sqrt{2\pi\sigma_2})^n}\frac{1}{f_{\sigma_1,\Lambda}(\mu_1)}\frac{1}{f_{\sigma_2,\Lambda}(\mu_2)}\sum_{t\in\Lambda} e^{-\frac{\|t-\frac{\sigma_1^2}{\sigma_1^2+\sigma_2^2}(y+(\frac{\sigma_2^2}{\sigma_1^2}\mu_1-\mu_2))\|^2}{2\frac{\sigma_1^2\sigma_2^2}{\sigma_1^2+\sigma_2^2}}}. \qquad (\star\star)$$

Обозначим $\rho_{\sigma,\mu}(x) = e^{-\frac{\|x-\mu\|^2}{2\sigma^2}}$, $\rho_{\sigma,\mu}(\Lambda) = \sum_{t\in\Lambda} e^{-\frac{\|t-\mu\|^2}{2\sigma^2}}$, $\tilde{\sigma} = \frac{\sigma_1\sigma_2}{\sqrt{\sigma_1^2+\sigma_2^2}}$ и $\tilde{\mu} = \frac{\sigma_1^2}{\sigma_1^2+\sigma_2^2}(y + (\frac{\sigma_2^2}{\sigma_1^2}\mu_1 - \mu_2))$.

$$(\star\star) = \frac{\rho_{\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)}{(\sqrt{2\pi}\sigma_1)^n(\sqrt{2\pi\sigma_2})^n}\frac{\rho_{\tilde{\sigma},\tilde{\mu}}(\Lambda)}{f_{\sigma_1,\Lambda}(\mu_1)f_{\sigma_2,\Lambda}(\mu_2)} = \rho_{\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)\frac{\rho_{\tilde{\sigma},\tilde{\mu}}(\Lambda)}{\rho_{\sigma_1,\mu_1}(\Lambda)\rho_{\sigma_2,\mu_2}(\Lambda)}. \qquad (\star\star\star)$$

Чтобы оценить полученное выражение с помощью ϵ нужно перейти к значению ρ на двойственной решётке. Переход к двойственной решётке осуществляется с помощью преобразования Фурье.

$$\begin{aligned}(\star\star\star) &\overset{\text{Лемма 3.1}}{=} \rho_{\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)\frac{V(\Lambda^\star)\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star)}{V(\Lambda^\star)\hat{\rho}_{\sigma_1,\mu_1}(\Lambda^\star)V(\Lambda^\star)\hat{\rho}_{\sigma_2,\mu_2}(\Lambda^\star)} \\ &= \rho_{\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)\frac{V(\Lambda)\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star)}{\hat{\rho}_{\sigma_1,\mu_1}(\Lambda^\star)\hat{\rho}_{\sigma_2,\mu_2}(\Lambda^\star)}.\end{aligned} \qquad (\star\star\star\star)$$

Преобразование Фурье гауссовской функции – это снова гауссовская функция $\hat{\rho}_{\sigma,\mu} = (\sqrt{2\pi}\sigma)^n\rho_{\frac{1}{\sigma},\mu}$. Свойство сдвига преобразования Фурье гласит, что если $h(x) = g(x+v)$, то $\hat{h}(w) = e^{2\pi i<w,v>}\hat{g}(w)$. Также выполняется $\rho_{\sigma,\mu}(x) = \rho_{\sigma,0}(x-\mu)$. Тогда

$$\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\lambda^\star) = (\sqrt{2\pi}\tilde{\sigma})^n e^{-2\pi i<\tilde{\mu},\lambda^*>}\rho_{\frac{1}{\tilde{\sigma}},0}(\lambda^\star).$$

$$\begin{aligned}\frac{1}{(\sqrt{2\pi}\tilde{\sigma})^n}\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star) = \frac{1}{(\sqrt{2\pi}\tilde{\sigma})^n}\sum_{\lambda^\star\in\Lambda^\star}\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\lambda^\star) &= \sum_{\lambda^\star\in\Lambda^\star} e^{-2\pi i<\tilde{\mu},\lambda^*>}\rho_{\frac{1}{\tilde{\sigma}},0}(\lambda^\star) \\ &= 1 + \sum_{\lambda^\star\in\Lambda^\star\setminus\{0\}} e^{-2\pi i<\tilde{\mu},\lambda^*>}\rho_{\frac{1}{\tilde{\sigma}},0}(\lambda^\star).\end{aligned}$$

$$|\frac{1}{(\sqrt{2\pi}\tilde{\sigma})^n}\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star) - 1| = |\sum_{\lambda^\star\in\Lambda^\star\setminus\{0\}} e^{-2\pi i<\tilde{\mu},\lambda^*>}\rho_{\frac{1}{\tilde{\sigma}},0}(\lambda^\star)| \le |\sum_{\lambda^\star\in\Lambda^\star\setminus\{0\}}\rho_{\frac{1}{\tilde{\sigma}},0}(\lambda^\star)| = \rho_{\frac{1}{\tilde{\sigma}},0}(\Lambda^\star\setminus\{0\}).$$

По определению коэффициента сглаживания и утверждению 3.12

$$|\frac{1}{(\sqrt{2\pi}\tilde{\sigma})^n}\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star) - 1| \le \rho_{\frac{1}{\tilde{\sigma}},0}(\Lambda^\star\setminus\{0\}) \le \epsilon. \qquad (3.18)$$

Аналогично

$$|\frac{1}{(\sqrt{2\pi}\sigma_1)^n}\hat{\rho}_{\sigma_1,\mu_1}(\Lambda^\star) - 1| \le \rho_{\frac{1}{\sigma_1},0}(\Lambda^\star\setminus\{0\}).$$

Так как $\frac{1}{\sigma_1} < \frac{1}{\tilde{\sigma}}$, то $\rho_{\frac{1}{\sigma_1},0}(\Lambda^\star\setminus\{0\}) < \rho_{\frac{1}{\tilde{\sigma}},0}(\Lambda^\star\setminus\{0\}) \le \epsilon$.

$$|\frac{1}{(\sqrt{2\pi}\sigma_1)^n}\hat{\rho}_{\sigma_1,\mu_1}(\Lambda^\star) - 1| \le \epsilon. \qquad (3.19)$$

Аналогично

$$|\frac{1}{(\sqrt{2\pi}\sigma_2)^n}\hat{\rho}_{\sigma_2,\mu_2}(\Lambda^\star)-1|\le\epsilon. \tag{3.20}$$

Обозначим

$$\gamma=\frac{\frac{1}{(\sqrt{2\pi}\tilde{\sigma})^n}\hat{\rho}_{\tilde{\sigma},\tilde{\mu}}(\Lambda^\star)}{\frac{1}{(\sqrt{2\pi}\sigma_1)^n}\hat{\rho}_{\sigma_1,\mu_1}(\Lambda^\star)\frac{1}{(\sqrt{2\pi}\sigma_2)^n}\hat{\rho}_{\sigma_2,\mu_2}(\Lambda^\star)}.$$

Из (3.18),(3.19) и (3.20) следует, что

$$1-4\epsilon\le\frac{1-\epsilon}{(1+\epsilon)^2}\le\gamma\le\frac{1+\epsilon}{(1-\epsilon)^2}\le1+12\epsilon.$$

Выразим дискретное гауссовское рапределение в виде

$$D_{\Lambda,\sigma,\mu}(\lambda)=\frac{\rho_{\sigma,\mu}(\lambda)}{\rho_{\sigma,\mu}(\Lambda)}\overset{\text{Лемма 3.1}}{=}\frac{\rho_{\sigma,\mu}(\lambda)}{V(\Lambda^\star)(\sqrt{2\pi}\sigma)^n\rho_{\frac{1}{\sigma},\mu}(\Lambda^\star)}=\frac{V(\Lambda)\rho_{\sigma,\mu}(\lambda)}{(\sqrt{2\pi}\sigma)^n\rho_{\frac{1}{\sigma},\mu}(\Lambda^\star)},\ \forall\lambda\in\Lambda.$$

Так как $\mathcal{Y}$ есть сумма двух точек решётки, то $\mathcal{Y}\in\Lambda$.

$$(\star\star\star\star)=\frac{\rho_{\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)}{(\sqrt{2\pi(\sigma_1^2+\sigma_2^2)})^n}V(\Lambda)\gamma=D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)\rho_{\frac{1}{\sqrt{\sigma_1^2+\sigma_2^2}},\mu_1+\mu_2}(\Lambda^\star)\gamma,$$

то есть $P_{\mathcal{Y}}(y)=D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)\rho_{\frac{1}{\sqrt{\sigma_1^2+\sigma_2^2}},\mu_1+\mu_2}(\Lambda^\star)\gamma$.

Тогда

$$\begin{aligned}|P_{\mathcal{Y}}(y)-D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)|&=D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)|1-\rho_{\frac{1}{\sqrt{\sigma_1^2+\sigma_2^2}},\mu_1+\mu_2}(\Lambda^\star)\gamma|\\&\le D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)|1-\gamma|\le D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)12\epsilon.\end{aligned}$$

$$\Delta(P_{\mathcal{Y}},D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2})=\sum_{y\in\Lambda}|P_{\mathcal{Y}}(y)-D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)|\le\sum_{y\in\Lambda}D_{\Lambda,\sqrt{\sigma_1^2+\sigma_2^2},\mu_1+\mu_2}(y)12\epsilon=12\epsilon$$

■

Теорема 3.5 утверждает, что статистическое расстояние ограничено уровнем плато решётки. Следовательно, если решётка Λ является криптостойкой, то есть её уровень плато ϵ_Λ экспоненциально убывает с увеличением размерности решётки, то распределение суммы дискретных гауссовских величин сколь угодно близко к дискретному гауссовскому распределению.

3.4.3 Несвязываемость

Рассмотрим i-й промежуточный узел. Он принимает сообщение $\mathcal{Y}_i^{in}=\sum\limits_j h_{ij}\mathcal{X}_j^{in}+\mathcal{U}_{r_i}$, где $\mathcal{X}_j^{in}=\lambda_{m_j}+\lambda_j$. Обозначим $\theta_{ij}=\alpha h_{ij}-a_{ij},\ a_{ij}\in\mathbb{Z}$. Если промежуточные узлы будут декодировать принятые сообщения по правилу (3.17), то

$$\mathcal{X}_i^{in}=Q_{\Lambda_r}(\alpha\mathcal{Y}_i^{in})\mathrm{mod}\Lambda_a=Q_{\Lambda_r}(\sum_j\alpha h_{ij}\mathcal{X}_j^{in}+\alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a$$

$$\overset{\text{Утв. 3.6}}{=} Q_{\Lambda_r}((\sum_j \alpha h_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a)) = Q_{\Lambda_r}((\sum_j a_{ij}\mathcal{X}_j^{in} + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a)$$

$$\overset{\text{Утв. 3.1}}{=} Q_{\Lambda_r}(((\sum_j a_{ij}\lambda_{m_j} + \sum_j a_{ij}\lambda_j)\mathrm{mod}\Lambda_a + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a)$$

$$\overset{\sum_j a_{ij}\lambda_j \in \Lambda_a, \text{ по Утв. 3.1}}{=} Q_{\Lambda_r}(((\sum_j a_{ij}\lambda_{m_j})\mathrm{mod}\Lambda_a + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a)$$

$$\overset{\text{Утв. 3.1}}{=} Q_{\Lambda_r}((\sum_j a_{ij}\lambda_{m_j} + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a)$$

$$\overset{\text{Утв. 3.6}}{=} Q_{\Lambda_r}(\sum_j a_{ij}\lambda_{m_j} + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a.$$

$\sum_j \theta_{ij}\mathcal{X}_j + \alpha\mathcal{U}_{r_i}$ – эквивалентный шум. Так как Λ_a – криптостойкая решётка, то по теореме 3.5 распределение $\sum_j \theta_{ij}\mathcal{X}_j$ близко к дискретному гауссовскому распределению, и следовательно, распределение эквивалентного шума по лемме 3.7 близко к непрерывному гауссовскому. Тогда

$$\mathcal{X}_i^{in} = Q_{\Lambda_r}(\sum_j a_{ij}\lambda_{m_j} + \sum_j \theta_{ij}\mathcal{X}_j^{in} + \alpha\mathcal{U}_{r_i})\mathrm{mod}\Lambda_a = \sum_j a_{ij}\lambda_{m_j}. \tag{3.21}$$

Таким образом, промежуточные узлы теряют «случайную» часть принятого сообщения. Передавать далее сообщение в виде (3.21) нельзя, так как это нарушает секретность и не дает возможности обеспечить несвязываемость.

Предлагается действовать следующим образом. Промежуточные узлы декодируют принятые сообщения по правилу (3.17), а затем снова кодируют по методу [79], описанному в пункте 3.3.2. В этом случае $\sum_j a_{ij}\lambda_{m_j}$ рассматривается i-м промежуточным узлом как информационная часть сообщения, и он выбирает новую «случайность» $\tilde{\lambda}_i$ с распределением $D_{\Lambda_a,\sigma_s,-\sum_j a_{ij}\lambda_{m_j}}$. Дальше передается точка $\mathcal{X}_i^{out} = \sum_j a_{ij}\lambda_{m_j} + \tilde{\lambda}_i$. Точка $\mathcal{X}_i^{out}$ принадлежит тому же смежному классу, что и принятая промежуточным узлом точка $\mathcal{X}_i^{in} = \sum_j a_{ij}\mathcal{X}_j^{in} = \sum_j a_{ij}\lambda_{m_j} + \sum_j a_{ij}\lambda_j$, так как определяет смежный класс информационная часть сообщения $\sum_j a_{ij}\lambda_{m_j}$, которая одинакова у $\mathcal{X}_i^{out}$ и $\mathcal{X}_i^{in}$. Так как точка $\tilde{\lambda}_i$ выбирается независимо от принятой точки, то точки $\mathcal{X}_i^{in}$ и $\mathcal{X}_i^{out}$ несвязываемы.

3.5 Анализ

3.5.1 Стойкость

Секретность является необходимым условием анонимности. Покажем это. Предположим, что злоумышленник умеет декодировать точки решётки Λ_r, то есть может восстанавливать точки

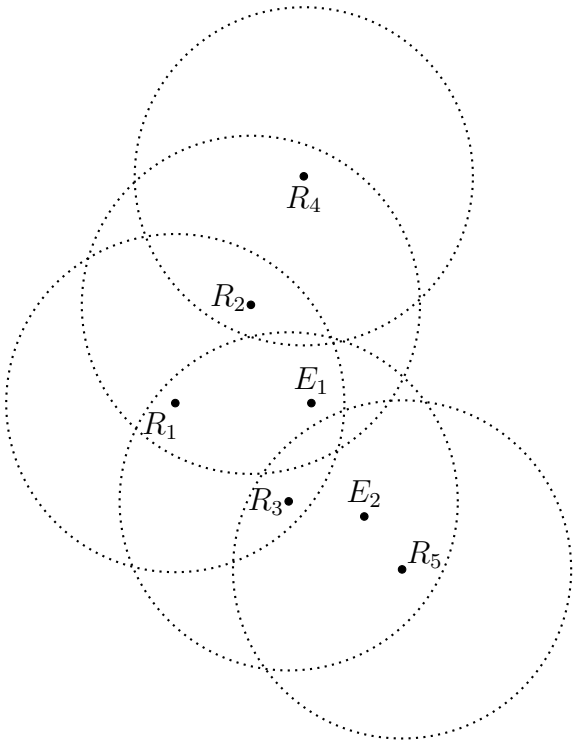


Рис. 3.9: Часть сети, прослушиваемой злоумышленником. Окружности вокруг узлов сети представляют собой границу слышимости сигналов этих узлов

$Q_{\Lambda_r}(\mathcal{Y}) = \mathcal{X} = \lambda_m + \lambda$. Пусть злоумышленник силами своего агента E_1 прослушал сообщение, передаваемое узлом R_1 (рис. 3.9), информационная часть которого есть линейная комбинация точек $\mathcal{X}_i = \lambda_{m_i} + \lambda_i \in \Lambda_r,\ i = 1, 2, \ldots, p$. Злоумышленник декодирует принятое сообщение с коэффициентом $a_{E_1} \in \mathbb{Z}$, получая $\mathcal{X} = a_{E_1} \sum\limits_i a_i \mathcal{X}_i$. Злоумышленник может обладать информацией о топологии сети, тогда ему известно, что это сообщение также слышали узлы R_2 и R_3. Злоумышленник будет прослушивать сообщения, отправляемые этими узлами в следующих временных слотах с помощью своих агентов E_1 и E_2. Пусть в следующем временном слоте передавал узел R_3. Декодирование сообщения от R_3 даст злоумышленнику $\hat{\mathcal{X}} = a_{E_2} \sum\limits_j a'_j \mathcal{X}'_j,\ j = 1, 2, \ldots, t$.

Первый случай. R_3 не получал в предыдущем временном слоте сообщений от других узлов кроме R_1, и $\hat{\mathcal{X}}$ является выходным сообщением для $\mathcal{X}$, то $t = p$, $a'_j = a_{R_3} a_i,\ \forall i = j$, где a_{R_3} – целочисленный коэффициент, с которым R_3 декодировал принятое сообщение и

$$\hat{\mathcal{X}} = \begin{cases} a_{E_2} a_{R_3} (\sum\limits_i a_i \mathcal{X}_i + \sum\limits_i a_i \lambda_{R_1}), \text{ для mod}\Lambda \text{ канала, } \lambda_{R_1} \text{ равномерно на } \Lambda_a \cap \mathcal{V}_0(\Lambda_s), \\ a_{E_2} a_{R_3} (\sum\limits_i a_i \mathcal{X}_i + \lambda_{R_1}), \text{ для канала общего вида, } \lambda_{R_1} \text{ имеет распределение } D_{\Lambda_a, \sigma_s, -\sum\limits_i a_i \lambda_{m_i}}. \end{cases}$$

$$\hat{\lambda}_m = \hat{\mathcal{X}} \text{mod} \Lambda_a = a_{E_2} a_{R_3} \sum_i a_i \lambda_{m_i},$$

$$\lambda_m = \mathcal{X} \text{mod} \Lambda_a = a_{E_1} \sum_i a_i \lambda_{m_i}.$$

Злоумышленник может проверить, содержат ли $\hat{\mathcal{X}}$ и $\mathcal{X}$ одинаковый набор информационных сообщений $\lambda_{m_i},\ i = 1, 2, \ldots, p$ с помощью проверочной матрицы $\mathbf{H}_r = \mathbf{G}_r^{-1}$ решётки Λ_r, где $\mathbf{G}_r$ – порождающая матрица решётки Λ_r. Так как $\lambda_{m_i} \in \Lambda_r$, то $\lambda_{m_i} = \mathbf{G}_r z_{m_i},\ z_{m_i} \in \mathbb{Z}^n$, $a_{(\cdot)} \in \mathbb{Z}$. Тогда

$$\mathbf{H}_r \hat{\lambda}_m = a_{E_2} a_{R_3} \sum_i a_i \mathbf{H}_r \lambda_{m_i} = a_{E_2} a_{R_3} \sum_i a_i \mathbf{G}_r^{-1} \mathbf{G}_r z_{m_i} = a_{E_2} a_{R_3} \sum_i a_i z_{m_i},$$
$$\mathbf{H}_r \lambda_m = a_{E_1} \sum_i a_i \mathbf{H}_r \lambda_{m_i} = a_{E_1} \sum_i a_i z_{m_i}.$$

$\mathbf{H}_r \hat{\lambda}_m$ и $\mathbf{H}_r \lambda_m$ являются целочисленными линейно зависимыми векторами. Из этого злоумышленник может сделать вывод, что $\mathcal{X}$ и $\hat{\mathcal{X}}$ передают один и тот же набор информационных сообщений $\lambda_{m_i},\ i = 1, 2, \ldots, p$. Это позволяет ему определить часть маршрута этого набора сообщений. Следующий за R_1 узел маршрута этих сообщений – это R_3. Далее злоумышленник может прослушивать сообщения узлов, которые принимают сообщения от R_3, т.е. узла R_5. Таким образом, можно проследить маршрут вплоть до получателя линейной комбинации сообщений $\lambda_{m_i},\ i = 1, 2, \ldots, p$.

Второй случай. Узел R_3 не получал в предыдущем временном слоте сообщений от других узлов кроме R_1, но в текущем слоте передаёт сообщение не от узла R_1. Тогда

$$\mathbf{H}_r \hat{\lambda}_m = a_{E_2} a_{R_3} \sum_j a'_j \mathbf{H}_r \lambda'_{m_i} = a_{E_2} a_{R_3} \sum_j a'_j z'_{m_j},$$
$$\mathbf{H}_r \lambda_m = a_{E_1} \sum_i a_i z_{m_i}.$$

Если $a_{E_1} a_{R_3} \sum_j a'_j z'_{m_j}$ и $a_{E_1} \sum_i a_i z_{m_i}$ линейно независимы, то злоумышленник сделает вывод, что R_3 не является следующим узлом маршрута интересующих его сообщений, и ему следует проанализировать таким же образом сообщения узла R_2. Если же они линейно зависимы, то злоумышленник сделает ошибочный вывод о том, что R_3 является следующим узлом маршрута.

Третий случай. Узел R_3 получал в предыдущем временном слоте сообщения от других узлов кроме R_1. Тогда $\hat{\mathcal{X}} = a_{E_2}(a_{R_3,1} \sum_i a_i \mathcal{X}_i + \sum_l a_{R_3,l} \mathcal{X}_l)$, где $\mathcal{X}_l$ представляет собой сообщение от другого узла. Этот случай эквивалентен случаю два.

Таким образом анонимность возможна пока сообщения передаются секретно.

3.5.2 Сложность

Сложность предлагаемого метода сравнима со сложностью операции декодирования.

В случае modΛ канала доминирующую сложность при вычислении выходного сообщения $\mathcal{X}_i^{out}$ имеет операция вычисления квантайзера Вороного, которая требуется и для генерации точки λ_2 равномерно распределённой в $\Lambda_a \cap \mathcal{V}_0(\Lambda_s)$ и для modΛ_s операции. Вычисление квантайзера Вороного является ключевой задачей кодирования и декодирования решётчатых кодов.

Она имеет экспоненциальную сложность. Наилучший известный алгоритм [84] имеет временную сложность $2^{2n+o(n)}$ и расход памяти $2^{n+o(n)}$, где n – размерность решётки.

Вычисление квантайзера Вороного упрощается для кубической решётки, т.е. для решётки вида $a\mathbb{Z}^n,\ a \in \mathbb{Z}$. В этом случае квантайзер вектора $x \in \mathbb{R}^n$ можно считать покоординатно. Произвольную решётку Λ с порождающей матрицей $\mathbf{G}$ можно трансформировать к кубической как $\mathbf{G}^{-1}\Lambda$. Тогда можно трансформировать решётку к кубической, найти квантайзер Вороного для кубической решётки и трансформировать его к первоначальной решётке Λ. Пусть необходимо вычислить $Q_\Lambda(x),\ x \in \mathbb{R}^n$. Вектор x может быть представлен в виде $x = \lambda + x_e,\ \lambda \in \Lambda$, т.е. $\lambda = \mathbf{G}z,\ z \in \mathbb{Z}^n$ и $x_e \in \mathcal{V}_0(\Lambda)$. Тогда $\mathbf{G}^{-1}x = z + \mathbf{G}^{-1}x_e$, а z – это точка решётки $\mathbb{Z}^n$. Следовательно, $Q_{\mathbb{Z}^n}(\mathbf{G}^{-1}x) = z$ и

$$\mathbf{G}Q_{\mathbb{Z}^n}(\mathbf{G}^{-1}x) = \mathbf{G}z = \lambda = Q_\Lambda(x). \tag{3.22}$$

Но равенство (3.22) выполняется только в том случае, если преобразование $\mathbf{G}$ сохраняет норму, то есть если из $\|x - \lambda\| \leq \|x - \lambda'\|$ следует $\|\mathbf{G}(x - \lambda)\| \leq \|\mathbf{G}(x - \lambda')\|$, что в свою очередь выполняется, если матрица $\mathbf{G}$ ортогональна.

Для канала общего вида основные вычислительные затраты приходятся на то, чтобы выбрать точку $\tilde{\lambda}$ согласно дискретному гауссовскому распределению. Наиболее известным алгоритмом, решающим эту задачу является [85] со сложностью $O(n^4 \log_2^2 b)$, где b – максимальная норма базисных векторов решётки.

3.6 Выводы

В этой главе диссертационной работы:

1) разработан метод обеспечения несвязываемости для частного случая сети, а именно, для сети с modΛ гауссовскими каналами;

2) показано, что метод обеспечивает совершенную несвязываемость в случае внешнего пассивного глобального злоумышленника;

3) обоснована возможность использования для сети метода семантической секретности, предложенного для гауссовского канала общего вида;

4) разработан метод несвязываемости сообщений для такой сети;

5) проанализированы стойкость и сложность предложенных методов.

Заключение

Диссертационная работа посвящена разработке и исследованию теоретико-информационных методов обеспечения несвязываемости. Сформулируем основные результаты, полученные в диссертации.

1. Построена теоретико-информационная модель анонимности, где анонимность определяется с помощью несвязываемости. Введено понятие совершенной несвязываемости.

2. Разработан теоретико-информационный метод обеспечения несвязываемости сообщений для цифрового когерентного сетевого кодирования, основанный на кодировании смежными классами для канала с подслушиванием второго типа. Дано теоретическое обоснование метода. Проведён анализ стойкости и сложности предложенного метода.

3. Разработан теоретико-информационный метод обеспечения несвязываемости сообщений для традиционной маршрутизации, основанный на кодировании смежными классами для канала с подслушиванием второго типа. Дано теоретическое обоснование метода. Проведён анализ стойкости и сложности предложенного метода.

4. Разработан теоретико-информационный метод обеспечения несвязываемости сообщений для аналогового сетевого кодирования, основанный на кодировании смежными классами для гауссовского канала с подслушиванием первого типа. Дано теоретическое обоснование метода. Проведён анализ стойкости и сложности предложенного метода.

Список литературы

[1] *Wyner A.D.* The wire-tap channel // The Bell System Technical Journal. –1975. – Vol. 54. – No 8. – P. 1355-1387.

[2] *Ozarow L.H., Wyner A.D.* Wire-Tap Channel II // Advances in Cryptology Lecture Notes in Computer Science. – 1985. – Vol. 209. – P. 33-50.

[3] *Csiszár I., Körner J.* Broadcast channels with confidential messages // IEEE Trans. Inf. Theory. – 1978. – Vol. 24. – No. 3. – P. 339-348.

[4] *Korener J., Marton K.* Comparision of two noisy channels // Topics in Information Theory, Coll. Math. Soc. J. Bolyai. – 1977. – No. 16. – P. 411-423.

[5] *Чисар И.* Почти независимость случайных величин и пропускная способность криптостойкого канала // Пробл. передачи информ. – 1996. – Т. 32. – Вып. 6. – С. 48-57.

[6] *Белакович И., Бохе Х., Зоммерфельд Й.* Результаты о конфиденциальности для составных каналов с подслушиванием // Пробл. передачи информ. – 2013. Том 49. – Вып. 1. – С. 83-111.

[7] *Leung-Yan-Cheong S.K., Hellman M.E.* The Gaussian Wire-Tap Channel // IEEE Trans. Inf. Theory. – 1978. – Vol. 24. – No. 4. P. 451-456.

[8] *Rouayheb S.Y.E., Soljanin E.* On wiretap networks II // Proc. IEEE Int. Symp. Inf. Theory. – 2007. – June. – P. 551–555.

[9] *Silva D., Kschischang R.* Univelsal Secure Network Coding via Rank-Metric Codes // IEEE Trans. Inf. Theory. – 2011. – Vol. 57. – No. 2. – P. 1124-1135.

[10] *Bellare M., Tessaro S., Vardy A.* A Cryptographic Treatment of the Wiretap Channel // https://arxiv.org/abs/1201.2205

[11] *Bellare M., Tessaro S., Vardy A.* Semantic Security for the Wiretap Channel // Advances in Cryptology - Crypto 2012 Proc. – 2012. – August. – P. 294-301.

[12] *Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.* Network information flow // IEEE Trans. Inf. Theory. – 2000. – Vol. 46. – No. 4. – P. 1204-1216.

[13] *Габидулин Э.М., Пилипчук Н.И., Трушина О.В.* Защита информации в телекоммуникационных сетях // Труды МФТИ. – 2013. – Т. 5. – №3. – С. 97-111.

[14] *Gabidulin E., Trushina O.* Anonymous and Secure Network Coding // Proc. of 7th International Workshop on Optimal Codes and Related Topics. – 2013. – September. – P. 85-90.

[15] *Трушина О.В., Габидулин Э.М.* Новый метод обеспечения анонимности и секретности в сетевом кодировании // Пробл. передачи информ. – 2015. – Т. 51. – Вып. 1. – С. 82-89.

[16] *Trushina O.* Anonymous Coherent Network Coding Against Active Adversary // Proc. of XV International Workshop on Algebraic and Combinatorial Coding Theory. – 2016. – June. – P. 278-283.

[17] *Габидулин Э.М., Трушина О.В.* Метод анонимной и секретной передачи данных в сетях с сетевым кодированием // Труды 56-й научной конференции МФТИ. – 2013. – Ноябрь. – С. 34-35.

[18] *Trushina O.* Towards to Anonymity in Physical-Layer Network Coding // Proc. of XIV International Workshop on Algebraic and Combinatorial Coding Theory. – 2014. – September. – P. 319-323.

[19] *Трушина О.В.* Обеспечение независимости передаваемых сообщений в гауссовском канале с подслушиванием // Труды 57-й научной конференции МФТИ. – 2014. – Ноябрь.

[20] *Трушина О.В.* Об анонимности в беспроводной сети // Труды конференции Инжиниринг & Телекоммуникации - En&T. – 2015. – Ноябрь. – С. 48-50.

[21] *Trushina O.* On the Anonymity of Physical-Layer Network Coding Against Wiretapping // Proc. of XV International Symposium "Problems of Redundancy in Information and Control Systems". – 2016. – September.

[22] *Chaum D.* Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms // Communications of the ACM – 1981. – V. 24 No. 2. – P. 84–88.

[23] *Pfitzmann A., Hansen M.* A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management // http://dud.inf.tudresden.de/literatur/Anon_terminology_v0.34.pdf – 2010.

[24] *Back A., Moller U., Stiglic A.* Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems // Proc. of the 4th International Workshop on Information Hiding. – 2001. – April. – P. 245-257.

[25] *Edman M., Yener B.* On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems // ACM Computing Surveys – 2009. – Vol. 42. – No. 1. – P. 1-35.

[26] *Ren J., Wu J.* Survey on anonymous communications in computer networks // Computer Communications – 2010. – Vol. 33, No. 4. – P. 420-431.

[27] *Chaum D.* The dining cryptographers problem: Unconditional sender and recipient untraceability // J. Cryptol.– 1988. – Vol. 1, No. 1. – P. 65-75.

[28] *Serjantov A., Dingledine R., Syverson, P.* From a trickle to a flood: Active attacks on several mix types // Proc. of the Information Hiding Workshop. – 2002. – October. – P. 36-52.

[29] *Kesdogan D., Egner J., Buschkes R.* Stop-and-go MIXes: Providing probabilistic anonymity in an open system // Proc. of Information Hiding Workshop. – 1998. – April. – P. 83-98.

[30] *Daz C., Serjantov A.* Generalising mixes // Proc. of Privacy Enhancing Technologies Workshop. – 2003. – March. – P. 18–31.

[31] *Danezis G., Sassaman L.* Heartbeat traffic to counter (n−1) attacks // Proc. of the Workshop on Privacy in the Electronic Society. – 2003. – October. – P. 89–93.

[32] *Goldschlag D.M., Reed M.G., Syverson P.F.* Hiding routing information // Proc. of the First International Workshop on Information Hiding. – 1996. – May. – P. 137-150.

[33] *Dingledine R., Mathewson N., Syverson P.* Tor: The second-generation onion router // Proc. of the 13th USENIX Security Symposium. – 2004. – August. – P. 303-320.

[34] https://www.torproject.org/

[35] *Waidner M.* Unconditional Sender and Recipient Untraceability in spite of Active Attacks // Proc. of Eurocrypt'89. – 1989. – April. – P. 302–319.

[36] *Sirer E.G., Polte M., Robson M.* Cliquenet: A Self-organizing, Scalable, Peer-to-peer Anonymous Communication Substrate // Cornell University, Computing and Information Science, Technical Report TR2001. – 2001.

[37] *Goel S., Robson M., Polte M., Sirer E.G.* Herbivore: A Scalable And Efficient Protocol For Anonymous Communication // Cornell University, Computing and Information Science, Technical Report TR2003-1890. – 2003.

[38] *Reiter M.K., Rubin A.D* Crowds: Anonymity for Web Transactions // ACM Transactions on Information and System Security. – 1998. – Vol. 1. – No. 1. – P. 66-92.

[39] *Wright M.K., Adler M., Levine B.N., Sheilds C.* The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems // ACM Transactions on Information and System Security (TISSEC). – 2004. – Vol. 7. – No. 4. – P. 489-522.

[40] *Levine B.N., Shields C.* Hordes: A Muplicast Based Protocol for Anonymity // Journal of Computer Security. – 2002. – Vol. 10. – No. 3. – P. 213-240.

[41] *Katti S., Cohen J., Katabi D.* Information Slicing: Anonymity Using Unreliable Overlays // Proc. of the 4th USENIX Symposium on Network Systems Design and Implementation. – 2007. – April. – P. 4-18.

[42] *Wang W., Duan G., Wang J., Chen J.* An Anonymous Communication Mechanism without Key Infrastructure based on Multi-paths Network Coding // Proc. of the 28th IEEE conference on Global telecommunications. – 2009. – November. – P. 832-837.

[43] *Zhang P., Jiang Y., Lin C., Lee P., Lui J.* ANOC: Anonymous Network-Coding-Based Communication with Efficient Cooperation // IEEE Journal on Selected Areas in Communications. – 2012. – Vol. 30. – No. 9. – P. 1738-1745.

[44] *Wang J., Wang J., Wu C., Lu K., Gu N.* Anonymous Communication with Network Coding against Traffic Analysis Attack // Proc. IEEE International Conference on Computer Communications INFOCOM'11. – 2011. – April. – P. 1008-1016.

[45] *Fan Y., Jiang Y., Zhu H., Chen J., Shen X.* Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks // IEEE Transactions on Wireless Communication. – 2011. – Vol. 10. – No. 3. – P. 834-843.

[46] *Zhang P., Jiang Y., Lin C., Fan Y., Shen X.* P-Coding: secure network coding against eavesdropping attacks // Proc. of the 29th IEEE International Conference on Computer Communications INFOCOM'10. – 2010. – March. – P. 1-9.

[47] *Reiter M.K., Rubin A.D.* Crowds: Anonymity for Web Transactions // ACM Transactions on Information and System Security. – 1998. – Vol. 1. – No. 1. – P. 66–92.

[48] *Tóth G., Hornák Z., Vajda F.* Measuring anonymity revisited // Proc. of 9th Nordic Workshop on Secure IT Systems. – 2004. – November. – P. 85–90.

[49] *Díaz C., Seys S., Claessens J., Preneel B.* Towards measuring anonymity // Pro. of the 2nd international conference on Privacy enhancing technologies. – 2002. – April. – P. 54-68.

[50] *Serjantov A., Danezis G.* Towards and Information Theoretic Metric for Anonymity // Proc. of the 2nd international conference on Privacy enhancing technologies. – 2002. – April. – P. 41-53.

[51] *Claub S., Schiffner S.* Structuring anonymity metrics // Proc. of Second ACM Workshop on Digital Identity Management. – 2006. – November. – P. 55–62.

[52] *Deng Y., Pang J., Wu P.* Measuring anonymity with relative entropy // Proc. of the 4th international conference on Formal aspects in security and trust. – 2006. – April. – P. 65-79.

[53] *Zhu Y., Bettati R.* Anonymity vs. information leakage in anonymity systems // Proc. of 25th IEEE International Conference on Distributed Computing Systems. – 2005. – June. – P. 514-524.

[54] *Edman M., Sivrikaya F., Yener B.* A combinatorial approach to measuring anonymity // Proc. of IEEE International Conference on Intelligence and Security. – 2007. – P. 356-363.

[55] *Gierlichs B., Troncoso C., Diaz C., Preneel B., Verbauwhede I.* Revisiting a Combinatorial Approach Toward Measuring Anonymity // Proc. of the 7th ACM Workshop on Privacy in the Electronic Society. – 2008. – October. – P. 111-116.

[56] *Berthold O., Federrath H., Köpsell S.* Web MIXes: A system for anonymous and unobservable Internet access // Proc. of International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. – 2000. – July. P. 115-129.

[57] *Bloch M., Laneman J.N.* On the Secrecy Capacity of Arbitrary Wiretap Channels // Proc. of 46th Annual Allerton Conference on Communication, Control, and Computing. – 2008. – September. – P. 818-825.

[58] *Shannon C.* Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949. – Vol. 28. – No. 4. – P. 656-715.

[59] *Сагалович Ю.Л.* Введение в алгебраические коды, Учебное пособие. - 2-е изд., перераб. и доп. – М.: ИППИ РАН, 2010. – 302 с.

[60] *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Пробл. передачи информ. – 1985. – Т. 21. – №1. – С. 3-16.

[61] *Gabidulin E., Ourivski A., Honary B., Ammar B.* Reducible Rank Codes and Applications to Cryptography // IEEE Trans. Inf. Theory. – 2003. – Vol. 49. – No. 12. – P. 3289-3293.

[62] *Ho T., Lun D.* Network Coding: An Introduction. – Cambridge University Press, 2008.

[63] *Ho T.*, *Médard M.*, *Koetter R.*, *Karger D.*, *Effros M.*, *Shi J.*, *Leong B.* A random linear network coding approach to multicast // IEEE Trans. Inf. Theory. – 2006. – Vol. 52. – No. 10. – P. 4413-4430.

[64] *Silva D., Kschischang F.R., Koetter R.* A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inf. Theory. – 2008. – Vol. 54. – No. 9. – P. 3951-3967.

[65] *Gabidulin E.M., Bossert M.* A family of algebraic codes for network coding // Proc. of IEEE International Symposium on Information Theory. – 2009. – June. – P. 2863-2866.

[66] *Rizzi A.* Statistical methods for Cryptography, Data Analysis and Classification // Proc. of the 6th Conference of the Classification and Data Analysis Group of the Societa Italiana di Statistica. – 2010. – P. 13-21.

[67] *Zamir R., Shamai (Shitz) S., Erez U.* Nested Linear/Lattice Codes for Structured Multiterminal Binning // IEEE Trans. Inf. Theory. – 2002. – Vol. 48. – No. 6. – P. 1250-1276.

[68] *Silva D., Kschischang F.R.* Universal Secure Error-Correcting Schemes for Network Coding // Proc. of IEEE International Symposium on Information Theory. – 2010. – June. – P. 2428-2432.

[69] *Габидулин Э. М., Пилипчук Н. И.* Лекции по теории информации. – М.: МФТИ, 2007. – 214 с.

[70] *Knuth D., Yao A.*. The complexity of nonuniform random number generation // Algorithms and Complexity: New Directions and Recent Results, Academic Press. – 1976.

[71] *Silva D., Kschischang F.R.* Fast encoding and decoding of Gabidulin codes // Proc. IEEE International Symposium on Information Theory. – 2009. – June. – P. 2858-2862.

[72] *Zhang S., Liew S., Lam P.* Hot topic: Physical-layer network coding // Proc. of 12th Annual Int. Conference on Mobile Computing and Networking. – 2006. – September. – P. 358-365.

[73] *Nazer B.,Gastpar M.*. Computing over multiple-access channels with connections to wireless network coding // Proc. of IEEE Int. Symposium on Information Theory. – 2006. –July. – P. 1354-1358.

[74] *Shomorony I., Avestimehr A.S* Worst-Case Additive Noise in Wireless Networks // IEEE Trans. Inf. Theory. – 2013. – Vol. 59. – P. 3833-3847.

[75] *Erez U., Zamir R.* Achieving $\frac{1}{2}\log(1+SNR)$ on the AWGN channel with lattice encoding and decoding // IEEE Trans. Inf. Theory. – 2004. – Vol. 50. – P. 2293-2314.

[76] *Zamir R.* Lattice Coding for Signals and Networks. – Cambridge University Press, 2014.

[77] *Nazer B., Gastpar M.* Compute-and-forward: Harnessing interference through structured codes // IEEE Trans. Inf. Theory. – 2011. – Vol. 57. – No. 10. – P. 6463-6486.

[78] *El Gamal A. A.* The Capacity of a Class of Broadcast Channels // IEEE Trans. Inf. Theory. – 1979. – Vol. 25. – No. 2. – P. 166-169.

[79] *Ling C., Luzzi L., Belfiore J.-C., Stehlé D.* Semantically secure lattice codes for the gaussian wiretap channel // IEEE Trans. Inf. Theory. – 2014. – Vol. 60. – P. 6399-6416.

[80] *Belfiore J.-C.* Lattice Codes for the Compute-and-Forward Protocol: The Flatness Factor // Proc. of IEEE Information Theory Workshop. – 2011. – October. – P. 1-4.

[81] *Oggier F., Solé P., Belfiore J.-C.* Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis // IEEE Trans. Inf. Theory. – 2016. – Vol. 62. – No. 10. – P. 5690-5708.

[82] *Regev O.*. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography // Journal of the ACM. – 2009. – Vol. 56. – No. 6. – P. 1-40.

[83] *Forutan V., Fischer R.F.H.* On the Security of Lattice-based Physical-layer Network Coding Against Wiretap Attacks // Proc. of 10th ITG International Conference on Systems, Communications and Coding. – 2015. – February. – P. 1-5.

[84] *Micciancio D., Voulgaris P.* A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations // Proc. of the forty-second ACM symposium on Theory of computing. – 2010. – June. – P. 351-358.

[85] *Klein P. N.* Finding the closest lattice vector when it's unusually close // Proc. of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms. – 2000. – January. – P. 937-941 .