

# Абстрактные анонимные сети

Коваленко Геннадий Александрович

**Аннотация.** Разработка абстрактных анонимных сетей, которым не важно расположение узлов, их количество, факт сокрытия IP-адресов и уровень централизованности системы, является новой и важной формой развития анонимизации трафика, которая позволяет внедряться в уже готовые, замкнутые и враждебные коммуникационные среды, оставляя при этом теоретически доказуемую анонимность. Подобные системы способны быстро восстанавливаться при массовых блокировках за счёт простоты возобновления своей работоспособности от одной лишь сетевой единицы. Свойство невосприимчивости к централизации способно порождать приложения, защищающие конфиденциальную информацию пользователей и анонимность их действий даже в полностью подконтрольных средах.

**Ключевые слова:** абстрактные анонимные сети; тайные каналы связи; децентрализованные сети; модель на базе обедающих криптографов; модель на базе очередей; модель на базе увеличения энтропии; мощность спама;

## Содержание

<b>1. Введение.....</b>	<b>1</b>
<b>2. Абстрактность сетевых коммуникаций.....</b>	<b>2</b>
<b>3. Примеры абстрактных анонимных сетей.....</b>	<b>5</b>
3.1. Модель на базе очередей.....	5
3.2. Модель на базе увеличения энтропии.....	14
3.3. Модель на базе обедающих криптографов.....	20
<b>4. Заключение.....</b>	<b>21</b>

## 1. Введение

Все анонимные сети базируются на двух идентифицирующих уровнях – сетевом и криптографическом. Сетевой уровень позволяет выстраивать маршрутизацию между узлами, более эффективно расходовать ресурсы частных ЭВМ и всей системы в целом. Криптографический уровень позволяет осуществлять анонимизацию субъектов посредством алгоритма запутывающей маршрутизации. Данный алгоритм часто становится связанным с сетевым уровнем непосредственно. Тем не менее, существует класс анонимных сетей, запутывающая маршрутизация которых позволяет полноценно отделяться от сетевых протоколов. Сама сетевая связь, в конечном итоге, становится лишь придатком общих коммуникаций, где все базовые функции идентификации и маршрутизации вбирает в себя криптографический уровень. При таком сценарии становятся незначимы такие факторы как расположение узлов в сети, сокрытие IP-адресов, число участников и уровень

централизованности системы. Данным сетям становится не важна как таковая коммуникационная среда, вследствие чего их анонимность может быть распространена далее на тайные каналы связи, располагаемые в заведомо враждебных и замкнутых системах. Во всей работе, вышеописанные системы будут именоваться абстрактными анонимными сетями.



**Рисунок 1.** Абстрактные анонимные сети являются подмножеством класса теоретически доказуемой анонимности

Абстрактные анонимные сети не могут не принадлежать сетям с теоретически доказуемой анонимностью [1]. Если взять обратное и предположить, что абстрактными могут быть скрытые сети без теоретически доказуемой анонимности, тогда они также должны уметь противостоять внешним и внутренним пассивным наблюдателям в замкнутом, незащищённом и враждебном окружении, как того предполагают тайные каналы связи. В таком пространстве внешний пассивный наблюдатель становится глобальным, а внутренний становится слиянием с глобальным, т.е. все функции отправления и получения информации будут проходить через единую, централизованную структуру (если брать самый худший и более вероятный сценарий образования тайных каналов связи). Такие суждения приводят к воссозданию теоретически доказуемой анонимности и к явному противоречию существования абстрактных скрытых сетей без теоретически доказуемой анонимности.

## 2. Абстрактность сетевых коммуникаций

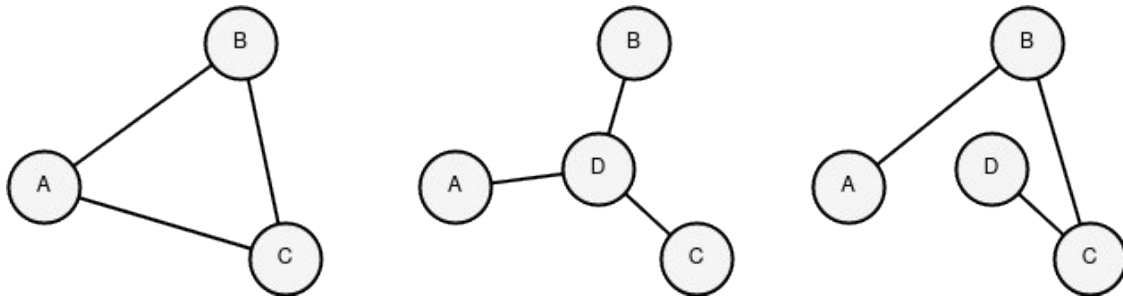
По умолчанию способ распространения всех абстрактных скрытых сетей сходится ко связи «все-ко-всем», то-есть когда каждый пользователь при генерации запроса отправляет свой пакет всем своим соединениям. Данное свойство связано с необходимостью минимального количества субъектов в системе для достижения анонимности с отсутствием противоречивости связей. Допустим, связь «один-к-одному» с двумя субъектами, заданная как  $(A \leftrightarrow B)$ , также является и фактической связью «все-ко-всем», и «все-к-одному», что приводит к противоречивой определённости. Такая же ситуация с возможностью представления связей «один-к-одному» и «все-к-одному» при помощи трёх субъектов. Поэтому минимальной структурой представления сетевых коммуникаций является связь «все-ко-всем» с тремя участниками сети.

В общем виде, существует всего три основных типа связей, как это представлено на *Рисунке 2*, в то время как все остальные соединения являются лишь их побочными гибридами.

- |                    |   |                       |
|--------------------|---|-----------------------|
| 1. «все-ко-всем»   | $(A \leftrightarrow B, B \leftrightarrow C, C \leftrightarrow A)$ | [распределённая],     |
| 2. «все-к-одному»  | $(A \leftrightarrow D, B \leftrightarrow D, C \leftrightarrow D)$ | [централизованная],   |
| 3. «один-к-одному» | $(A \leftrightarrow B, B \leftrightarrow C, C \leftrightarrow D)$ | [децентрализованная]. |

Во-первых, стоит сказать, что все приведённые выше связи являются одноранговыми, в том числе и связь централизованная. Данные соединения рассматриваются в вакууме абстрактной сети, а следовательно, все они априори предполагают одноранговую, peer-to-peer модель. Разделение связей рассматривает лишь расположение и сочетание субъектов относительно друг друга, а не дополнительную нагрузку, повышение прав или разделение полномочий.

Во-вторых, стоит заметить, что связи «все-к-одному» и «один-к-одному» схожи между собой куда больше, чем отдельно каждое из представленных со связью «все-ко-всем». Для полного представления распределённой связи достаточно трёх узлов, в то время как для двух оставшихся необходимо уже четыре узла. Связано это с тем, что если представить децентрализованную связь при помощи трёх субъектов, то результатом такого преобразования станет связь централизованная, и наоборот, что говорит об их родстве, сходстве и слиянии более близком, нежели со связью распределённой.



**Рисунок 2.** Связи: «все-ко-всем», «все-к-одному», «один-к-одному» (слева направо)

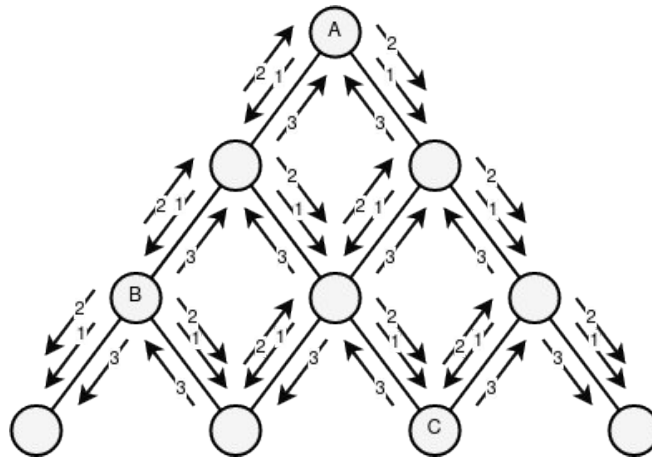
В-третьих, централизованная связь по своей концепции распространения информации стоит ближе к связи распределённой, нежели связь децентрализованная. Сложность распространения объекта между истинными субъектами информации в распределённых и централизованных системах равна  $O(1)$ , в то время как в децентрализованных сложность равна  $O(N)$ .

В-четвёртых, по критериям отказоустойчивости децентрализованная связь стоит ближе к распределённой, нежели связь централизованная. В связи «все-ко-всем», при удалении одного субъекта, сеть остаётся целостной и единой. В связи «один-к-одному», при удалении одного субъекта, сеть может разделиться на  $N$  децентрализованных сетей. В связи «все-к-одному», при удалении одного субъекта, сеть может прекратить своё существование вовсе.

Таким образом, схожесть и однородность связей можно представить как (децентрализованная  $\leftrightarrow$  централизованная)  $\leftrightarrow$  (централизованная  $\leftrightarrow$  распределённая)  $\leftrightarrow$  (распределённая  $\leftrightarrow$  децентрализованная). При цикличности трёх элементов, инициализируется общий эквивалент представленный в формации соединений «все-ко-всем».

Далее, если предположить, что существует четыре субъекта  $\{A, B, C, D\}$  со связью «все-к-одному», где центральным узлом является точка  $D$ , то анализ безопасности абстрактной анонимной сети будет сводиться к осмотру действий от узла  $D$  ко всем остальным субъектам и от любого другого узла к субъекту  $D$ . В одном случае будет происходить прямая

широковещательная связь, в другом же случае, будет происходить передача сообщения для последующей множественной репликации.



**Рисунок 3.** Маршрутизация пакета на базе абстрактной анонимной сети из 10 узлов, где *A* - отправитель, *B* - маршрутизатор, *C* - получатель

Если предположить, что субъект *D* не способен генерировать информацию, а создан исключительно для её ретранслирования, то это эквивалентно его отсутствию как таковому. Действительно, если пакет имманентен в своём проявлении (не выдаёт никакую информацию о субъектах), то все действия внутреннего узла *D* тождественны внешнему наблюдателю, а как было утверждено ранее, абстрактная сеть невосприимчива к такому виду деанонимизации. Следовательно, узел *D* становится словно фантомом, ретранслирующим субъектом не влияющим на безопасность и анонимность сети, базируемой на связи «все-к-одному». Из этого также следует, что абстрактная система может применяться и в тайных каналах связи, где безопасность приложения выстраивается в заведомо подконтрольной, враждебной и централизованной инфраструктуре.

Теперь, если субъект *D* способен генерировать информацию, то создавая сеть и имплюзируя её в себя, субъект сам становится сетью, в которой он априори соединён со всеми, что приводит это суждение ко связи «один-ко-всем». Связь же «все-ко-всем», состоит из множества связующих «один-ко-всем» относительно каждого отдельного субъекта, коим и является узел *D*, а это, в свою очередь приводит к классическому (ранее заданному) определению абстрактной анонимной сети. Таким образом, связь «все-к-одному» внутри себя уже содержит логическую составляющую связи «все-ко-всем» через которую и доказывается её безопасность.

Доказать безопасность связи «один-к-одному» возможно через неопределённость посредством её слияния со связью «все-к-одному», которое определяется при трёх участниках сети. Такое свойство неоднородности и неоднозначности предполагает, что сеть становится одновременно и централизованной, и децентрализованной. Следовательно, доказав ранее безопасность связи «все-к-одному», автоматически доказывается и безопасность связи «один-к-одному» для конкретно заданного случая.

Далее, если предположить, что существует четыре субъекта  $\{A, B, C, D\}$  со связью «один-к-одному», то базируясь на итеративности передачи информации в децентрализованных системах, можно декомпозировать любую модель в более замкнутую. Таким образом, сеть  $\{A, B, C, D\}$  фактически может расщепиться на две подсети  $\{A, B, C\}$  и  $\{B, C, D\}$ , мостом которых являются субъекты  $\{B, C\}$ . Каждая отдельная подсеть представляет собой ту же неопределённость, внутри которой присутствует централизованная

система. В результате, безопасность связи «один-к-одному» сводится ко связи «все-к-одному», и как следствие, ко связи «все-ко-всем».

Таким образом, вне зависимости от типа соединений, абстрактная скрытая сеть будет оставаться безопасной, даже при условии существования единственного сингулярного сервера, связывающего всех клиентов между собой. Простота построения централизованной системы в абстрактной анонимной сети приводит противоречиво к выражению истинной отказоустойчивости, а также к живучести подобных коммуникаций, регенерирующих лишь от одной сетевой единицы. Данное свойство, в большей мере, отличает абстрактные анонимные сети от всех других скрытых сетей.

### 3. Примеры абстрактных анонимных сетей

Одним из возможных способов (как шагов) построения таковых систем является необходимость в доказуемой устойчивости системы по отношению хотя бы к одному из наблюдателей, будь то внешнему или внутреннему. При этом в качестве внешнего берётся наивысшая форма в лице глобального наблюдателя, а в качестве внутреннего берутся узлы, заполняющие всю сеть с определённой минимальной условностью по количеству несвязанных между собой узлов.

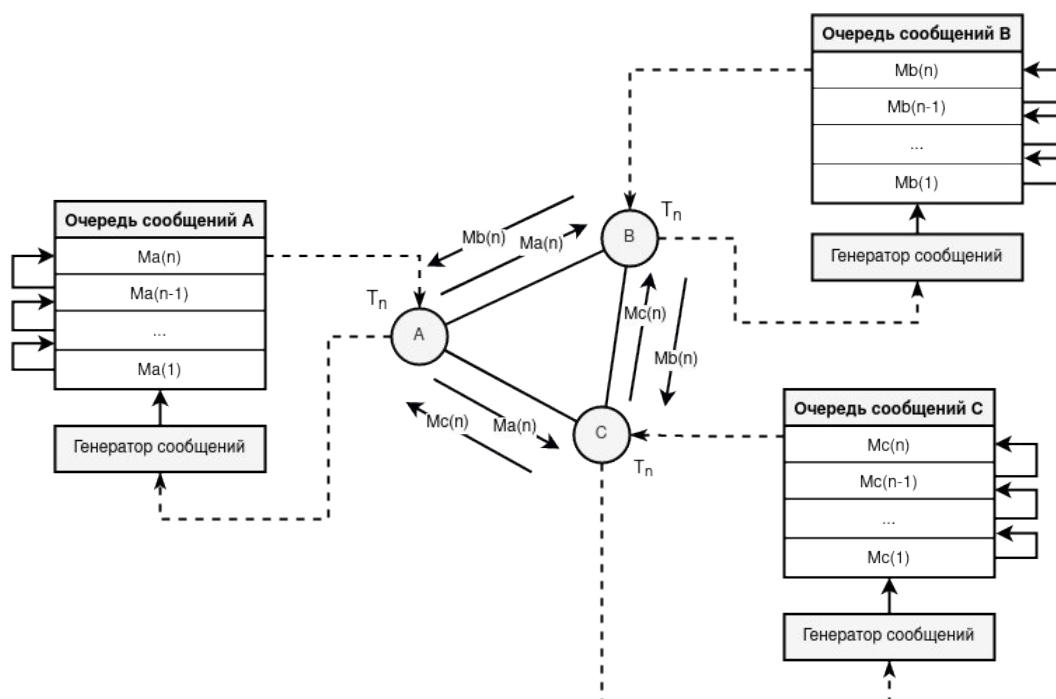
Простота системы является также важным качеством теоретически доказуемой анонимности. Если система будет иметь массу условностей, то даже при теоретической её доказуемости, практическая реализация может составить огромное количество трудностей, ошибок или неправильных использований, что приведёт к фактической дискредитации самой теории, и таковая анонимность в конечном счёте останется лишь теоретической.

#### 3.1. Модель на базе очередей

Одной из самых простых возможных реализаций абстрактной системы является использование очередей генерации пакетов в сети. Для начала предположим, что необходимо защититься от внешнего глобального наблюдателя. Также предположим, что существует три узла в сети  $\{A, B, C\}$ , где один из них отправитель информации, а другой – получатель. Целью атакующего становится сопоставление факта отправления с инициатором и/или получения с сервисом связи (получателем). В идеальной системе (теоретически доказуемой) вероятность обнаружения правильного запроса составит  $1/3$ . Ровно такая же картина должна быть с фактом ответа на запрос. В сумме при трёх участниках и при условии ИЛИ факт обнаружения должен быть равен  $2/3$  (не имеет значения запрос это или ответ). При существовании  $N$  узлов несвязанных между собой общими целями и интересами, вероятность становится равной  $2/N$ . Итоговая система должна удовлетворять данным свойствам.

Предположим далее, что необходимо защититься от  $q$ -ого количества внутренних наблюдателей системы из количества  $q + |\{A, B, C\}|$  узлов, где известно, что узел  $C$  – не связанный в сговоре маршрутизатор для одного из узлов  $A$  или  $B$ . Если внутренний наблюдатель становится пассивным, то спектр его действий ограничивается внешним наблюдением с  $q$ -ым охватом сети, при условии, что пакет не выдаёт никакой информации об отправителе или получателе. Таким образом, в данном контексте необходимым является рассмотрение активных внутренних нападений, где субъект-атакующий становится способным генерировать самостоятельно пакеты и быть отправителем информации к определённой точке назначения. Целью атакующего становится сопоставление факта отправления ответа из множества  $\{A, B\}$  с конкретным его элементом. В идеальной системе

(теоретически доказуемой) вероятность обнаружения правильного ответа составит  $1/2$ . При существовании  $N$  узлов несвязанных между собой общими целями и интересами, вероятность становится равной  $1/N$ . Итоговая система должна удовлетворять данным свойствам.



**Рисунок 4.** Схема абстрактной анонимной сети на базе очередей со стороны внешнего глобального наблюдателя

Если предположить, что существует сговор пассивного внешнего и активного внутреннего наблюдателей, то условие и цель атакующих полностью становится аналогична цели внутреннего наблюдателя, где в идеальной системе (теоретически доказуемой) ровно также вероятность обнаружения ответа должна составить  $1/2$ . При существовании  $N$  узлов несвязанных между собой общими целям и интересами, вероятность должна становиться равной  $1/N$ . Итоговая система должна удовлетворять данным свойствам.

Работа системы на базе очередей может сводиться к следующему протоколу на основе 10 пунктов, которые полностью (за исключением сговора активных наблюдателей) обеспечивают замкнутость и безопасность системы:

1. Каждый субъект сети должен выстроить период генерации пакета равный  $T_n$ , где  $n \in Q$ ,  $n$  – статичная величина периода. Иначе становится эффективна атака со стороны внутреннего наблюдателя. Несогласованность константного числа  $T_n$  с другими участниками сети приведёт к возможности разграничения субъектов по подмножествам с разными периодами генераций.
2. Каждый субъект сети выстраивает период равный  $T_n$  полностью локально, без кооперирования с другими субъектами сети. Это условие является лишь упрощением системы, само кооперирование или его отсутствие не приведёт к нарушению протокола, потому как предполагается, что сама генерация пакетов, а конкретно время начала генерации, не является секретом.

3. Каждый действующий субъект сети выставляет минимум одного существующего пользователя в роли маршрутизирующего узла для поддержания анонимности. Причисление маршрутизатора в сговор атакующих приведёт к деанонимизации субъектов, использующих данного промежуточного участника. Поэтому, в практическом применении для снижения рисков связанных с деанонимизацией субъектов посредством контроля ретранслятора, необходимо выбирать сразу несколько маршрутизирующих узлов, формируя тем самым цепочку нод и повышая мощность анонимности.

4. Каждый действующий субъект сети знает период и время генерации нового пакета на маршрутизирующем узле. Такое условие необходимо для предотвращения от атак направленных на нестабильные системы (как будет показано далее) с учётом существующего сговора внешних и внутренних наблюдателей.

5. Каждое сообщение зашифровывается монолитным криптографическим протоколом [2] с множественным туннелированием и проходит сквозь маршрутизирующие узлы. Такое свойство приведёт к сильному разрыву связей между объектом и его субъектами, а также между идентификацией сетевой и криптографической.

6. Каждый субъект хранит все свои сообщения, готовые к отправлению по сети, в очереди. Помимо очереди субъект должен содержать автодополняющийся пул ложных сообщений. Данное свойство необходимо для пункта 7.

7. Если на момент  $T_{ni}$  очередь пуста, где  $i \in N$ ,  $i$  – номер периода, то-есть не существует ни запроса, ни ответа, ни маршрутизации, то отправляется сообщение из пула ложных сообщений. При таком случае, данное сообщение фактически никто не получает.

8. Если приходит сообщение представляющее собой маршрутизацию, то оно ложится в очередь и при наступлении локального времени  $T_{ni}$  отправляется по сети. Пункт 5 обеспечивает несвязность объекта с его субъектами, поэтому при получении сообщения-маршрутизации, промежуточный принимающий узел увидит только факт маршрутизации.

9. При необходимости отправить запрос, субъект сначала анализирует текущее время с периодом маршрутизатора, с целью отправить сообщение на второй итерации периода маршрутизирующего узла. Если ещё не прошла собственная итерация периода, то перед запросом в очередь вставляется ложное сообщение, данный запрос отправляется по сети. Пункт 3 обеспечивает несвязность идентификации сетевой и криптографической, что не даёт отправителю никакой информации о получателе, кроме его публичного ключа.

10. При необходимости отправить ответ, субъект сначала анализирует текущее время с периодом маршрутизатора, с целью отправить сообщение на второй итерации периода маршрутизирующего узла. Если ещё не прошла собственная итерация периода, то перед ответом в очередь вставляется ложное сообщение, данный ответ отправляется по сети. Пункт 3 обеспечивает несвязность идентификации сетевой и криптографической, что не даёт получателю никакой информации об отправителе, кроме его публичного ключа.

Явным недостатком данной архитектуры становится подверженность атакам отказа в обслуживании (DDoS), как для конкретного субъекта, перегружая его очередь сообщениями, так и для всей сети. Связано это с тем, что в основе системы используются очереди,

сохраняющие и накапливающие сообщения, а также слепая маршрутизация, порождающая наибольшую несвязанность объекта с его субъектами за счёт полного распространения информации по всем участникам сети.

В любом случае преднамеренные атаки на сеть с целью отказа в обслуживании можно предотвратить проверяемостью на принадлежность субъектов к периоду генерации сообщений, но при всё большем расширении сети сами её участники станут давлением и причиной ухудшения производительности. Причиной такого исхода становится линейная увеличивающаяся нагрузка на сеть  $O(N)$  прямо пропорционально количеству действующих узлов  $N$  в сети. Иными словами, каждый субъект должен будет обрабатывать в  $T_n$  период  $N-1$  пакетов, постоянно расшифровывая их, что и становится достаточно ресурсозатрачиваемой операцией.

Тем не менее, в выстроенной системе становится достаточно легко доказать невозможность атаки со стороны внешнего наблюдателя, анализирующего дифференциальность сети. Если каждый субъект соблюдает генерацию пакета по локальному периоду (даже гипотетически с разными значениями  $T_n$ ), то становится невозможным установление факта отправления, получения, маршрутизации или ложной генерации, потому как наблюдатель, в конечном счёте, способен лишь видеть определённые зашифрованные сообщения генерируемые каждый промежуток времени равный  $T_n$ . Также, если внешним наблюдателем будут блокироваться определённые субъекты информации без непосредственного кооперирования со внутренним атакующим, то кардинально данный подход ситуации не изменит.

Атака внутренних наблюдателей с приведённым выше условием является качественно более сложной и мощной (даже относительно большинства внутренних нападений на практике), потому как  $q$  субъектов контролируют всю сеть за исключением трёх субъектов, а следовательно атакующие фактически являются не только внутренними наблюдателями, но и в массе своей монолитным глобальным наблюдателем. В качестве упрощения доведём нападения до теоретически возможной комбинации, в отображении сговора внешних и внутренних наблюдателей. Аудит будет базироваться на 10 пункте, когда субъекту должен сгенерироваться ответ на отправленный запрос. При анализе системы может встретиться два разных случая – частный (а) (наиболее благоприятный в определении анонимности) и общий (б) (дающий больший простор действий для нападающих).

Частный случай удобно рассматривать на примере основных подходов к деанонимизации и методов их предотвращения. Общий же случай более реален в настоящем мире, потому как частный неустойчив к отказам в обслуживании (если субъект переподключится, то изменится сдвиг периода) и требует из-за этого постоянного кооперирования субъектов между собой по времени (чтобы сама генерация информации была одновременной). Таковые условия поведения частного случая делают общий более приоритетным в анализе практической анонимности, потому как он становится «стабильным» за счёт невозможности своего дальнейшего ухудшения.

а) Частный случай. Предположим, что существует крайне стабильная система при которой каждый узел из множества  $\{A, B, C\}$  выставил в один и тот же промежуток времени значение равное  $T_n$  без отставания по времени относительно всех остальных участников сети. Все участники генерируют запрос секунда в секунду каждые  $T_{ni}$  по периоду. Предположим, что  $T_n = 3$ , тогда генерацию можно представить в виде Таблицы 1.

	$T_{n1-2}=t_1$	$T_{n1-1}=t_2$	$T_{n1}=t_3$	$T_{n2-2}=t_4$	$T_{n2-1}=t_5$	$T_{n2}=t_6$	$T_{n3-2}=t_7$	$T_{n3-1}=t_8$	$T_{n3}=t_9$
A			+			+			+



В			+			+			+
С			+			+			+

**Таблица 1.** Стабильная система со множеством участников  $\{A, B, C\}$  и  $T_n = 3$

Если отсутствует маршрутизация от субъекта  $C$ , то легко определимым становится вычисление истинного субъекта генерирующего настоящее сообщение. И действительно, если существует сговор внутреннего и внешнего наблюдателей, то возможен сценарий, при котором внутренний наблюдатель, в роли инициатора, генерирует сообщение и отправляет его одному из участников  $\{A, B\}$ . Спустя период  $T_n$  (при условии, что у получателя не существует сообщений в очереди) инициатор получает ответ, предварительно сохраняя его зашифрованную версию. Далее внутренний наблюдатель обращается к внешнему с зашифрованной версией сообщения, тот в свою очередь по своим записям проверяет где впервые был создан таковой пакет. Узел на котором появилось впервые подобное сообщение и является истинным субъектом информации в лице получателя.

Теперь предположим, что маршрутизация субъекта  $C$  существует. Если внутренний наблюдатель хочет раскрыть субъектов  $\{A, B\}$ , то можно предположить, что ему необходимо каким-либо образом обойти ретрансляцию субъекта  $C$ . Но исключение узла  $C$  из сети не является решением, потому как прекратится вся последующая связь с субъектом  $A$  или  $B$ . Другим способом раскрытия (и куда более продуктивным) является уже исключение одного субъекта из множества  $\{A, B\}$ , иными словами блокировка участника сети на определённый период времени  $mT_n$ . Тогда в таком случае активный внешний наблюдатель блокирует одного из субъектов  $\{A, B\}$ , после этого активный внутренний наблюдатель посылает запрос на одного из субъектов множества  $\{A, B\}$ . Если отправитель получает ответ, значит истинным получателем информации является не исключённый участник, в противном случае – исключённый.

Для предотвращения активных атак со стороны сговора внешних и внутренних наблюдателей необходимо добавить дополнительный (но не единственно возможный) 11<sub>1</sub> пункт, который представляет новую псевдо-роль субъектов в качестве контролирующих узлов. Такая атака приводит к невозможности деанонимизации субъектов посредством частичного блокирования, потому как её следствием станет взаимоблокировка субъектов. Тем не менее добавление данного пункта скажется на том, что сама сеть выйдет из класса абстрактных анонимных сетей, потому как добавится необходимость в поточном распространении информации на базе прямых соединений.

11<sub>1</sub>. Каждый действующий субъект сети выставляет минимум одного существующего пользователя в роли контролирующего узла для предотвращения от активных атак методом исключения участников системы. Суть такого пользователя в понимании его существования. Если связь с подобным субъектом будет разорвана, то все последующие действия автоматически прекращаются. Само соединение функционирует за пределами механизма очередей, что, тем не менее, не приводит к снижению уровня анонимности, потому как все субъекты начинают подчиняться этому правилу односторонне (в такой концепции не существует функций типа запрос/ответ, существуют только поточные уведомления своего присутствия).

Хоть теоретически сама атака становится невозможной, но в практическом смысле и в долгосрочном наблюдении она более чем реальна. Связано это с тем, что одноранговая архитектура как таковая приводит к постоянному и динамичному изменению связей между

субъектами. Это в свою очередь может приводить к исключениям групп субъектов связанных контролирующими узлами, потому как последние обязаны быть действующими и настоящими участниками системы, в отличие от маршрутизирующих узлов.

Ещё одним возможным решением вышеописанной проблемы может стать использование доверенных соединений между участниками сети. Такой подход ограничивает действия активных внутренних наблюдателей и за счёт данного свойства позволяет снизить риски деанонимизации, а также сохранить абстрактность системы (по сравнению с пунктом 11<sub>1</sub>).

11<sub>2</sub>. Каждый действующий субъект сети выстраивает связи с другими участниками, основываясь на субъективности к уровню доверия, устанавливая и редактируя белый список на своей стороне. Чтобы успешно подключиться к сети такого рода, субъекту необходимо стать доверенным узлом, то есть пользователем, которому кто-либо доверяет. Сложность исполнения атаки на подобную сеть будет сводиться к сложности встраивания подчиняемых узлов, потому как каждый получатель информации, в конечном итоге, должен будет заранее устанавливать список возможных отправителей.

Сети с таким свойством именуется friend-to-friend (F2F) сетями [3]. Естественным недостатком является малая экспансия, как возможность масштабирования системы. С другой стороны, как раз такое качество позволяет дополнительно (и довольно эффективно) сдерживать недостатки самой структуры, когда увеличивающееся количество субъектов приводит линейно к регрессу производительности системы. В общем представлении такой метод защиты достаточно эффективен против внутренних активных наблюдателей (особенно с практической точки зрения), но теоретически является более сложной моделью. Анонимность такого случая начинает базироваться на гипотетически большем количестве связей между участниками, чем при выстраивании константно заданного количества маршрутизирующих узлов, что и приводит к дополнительным рискам деанонимизации субъектов.

Также ещё одним возможным решением может стать синтез подходов, что закономерно объединит не только положительные, но и отрицательные стороны этапов 11<sub>1</sub> и 11<sub>2</sub>. В следствии такого соединения система перестанет быть абстрактной (за счёт необходимости в поточном поддержании соединений), появится свойство малой экспансии (за счёт принадлежности к F2F-сети) и увеличится сложность практической реализации (за счёт, соответственно, синтеза двух подходов). Тем не менее, теоретическая безопасность выйдет на более лучший уровень, потому как если один из доверенных субъектов станет скомпрометированным, то останется дополнительный слой защиты в лице маршрутизаторов, и наоборот.

б) Общий случай. Предположим, что существует нестабильная система при которой каждый узел из множества  $\{A, B, C\}$  выставил в разный промежуток времени значение равное  $T_n$  с отставанием по времени относительно всех остальных участников сети. Все участники генерируют запрос в разные секунды, но также сохраняя локальный период равный  $T_n$ . Предположим, что  $T_n = 3$ , тогда генерацию можно представить в виде Таблиц 2, 3, 4 относительно расположения субъекта  $C$  к другим участникам.

	$T_{n-2}=t_1$	$T_{n-1}=t_2$	$T_{n1}=t_3$	$T_{n2-2}=t_4$	$T_{n2-1}=t_5$	$T_{n2}=t_6$	$T_{n3-2}=t_7$	$T_{n3-1}=t_8$	$T_{n3}=t_9$
A		+			+			+	
B			+			+			+

C	+			+			+		
---	---	--	--	---	--	--	---	--	--

**Таблица 2.** Нестабильная система со множеством участников  $\{A, B, C\}$  и  $T_n = 3$ , где узел  $C$  находится в начале генерации

	$T_{n-2}=t_1$	$T_{n-1}=t_2$	$T_{n1}=t_3$	$T_{n2-2}=t_4$	$T_{n2-1}=t_5$	$T_{n2}=t_6$	$T_{n3-2}=t_7$	$T_{n3-1}=t_8$	$T_{n3}=t_9$
A	+			+			+		
B			+			+			+
C		+			+			+	

**Таблица 3.** Нестабильная система со множеством участников  $\{A, B, C\}$  и  $T_n = 3$ , где узел  $C$  находится в середине генерации

	$T_{n-2}=t_1$	$T_{n-1}=t_2$	$T_{n1}=t_3$	$T_{n2-2}=t_4$	$T_{n2-1}=t_5$	$T_{n2}=t_6$	$T_{n3-2}=t_7$	$T_{n3-1}=t_8$	$T_{n3}=t_9$
A		+			+			+	
B	+			+			+		
C			+			+			+

**Таблица 4.** Нестабильная система со множеством участников  $\{A, B, C\}$  и  $T_n = 3$ , где узел  $C$  находится в конце генерации

В качестве упрощения и абстрагирования предположим, что ни для какого субъекта не существует контролирующего участника или F2F-соединений, а следовательно и пунктов  $11_1$  и  $11_2$  как таковых. Существуют только субъекты  $\{A, B\}$  (один из которых является настоящим получателем) и постоянный маршрутизатор  $C$ . Основной целью анонимизации в нестабильных коммуникациях становится сведение действий субъекта  $A$  к аналогичным действиям субъекта  $B$ , и наоборот, посредством маршрутизатора  $C$ . Действительно, если  $C$  станет замыкающим узлом в момент времени  $T_{ni}$  при ответе любого субъекта множества  $X$ , то возникнет максимальная неопределённость равная  $1/|X|$ .

Анализируя сетевые коммуникации в нестабильных системах внешний наблюдатель способен сопоставлять для каждого субъекта его период равный  $T_n$  и сдвиг относительно определённого субъекта. В сговоре со внутренним наблюдателем появляется возможность деанонимизации субъекта на базе приведённого сдвига. Предположим, что игнорируется условие пунктов 9 и 10 с необходимостью генерировать пустое сообщение на основе периодов маршрутизирующего узла. Далее, пусть существует сеть на базе Таблицы 2, где внутренний наблюдатель располагает всеми сведениями полученными от внешнего атакующего и на основе этого генерирует сообщение в момент времени  $T_{n1}$  и отправляет его по сети. Если будет получен ответ в момент  $T_{n1+1} = T_{n2-2}$  от маршрутизатора  $C$ , то это говорит только о том, что получателем сообщения является участник  $B$ , потому как субъект  $A$  становится способным выдать ответ маршрутизирующему узлу только в период  $T_{n1+2} = T_{n2-1}$ , по причине его умышленного пропуска в момент  $T_{n1-1}$  атакующей стороной. Такой вид атаки приводит к полной деанонимизации субъектов.

Предотвращением атаки является отправление истинного пакета на вторую итерацию периода маршрутизирующей стороны (относительно текущего времени). Теперь репродуцируем вышеописанную атаку на систему с таким условием. Также предположим, что сетью является система на базе Таблицы 2. Если атакующий сгенерирует сообщение в момент времени  $T_{n1}$ , то получит ответ только в момент  $T_{n3-2}$ . Получателем в такой системе может оказаться любой из множества  $\{A, B\}$ , потому как ответ может быть отправлен как в

момент времени  $T_{n2-1}$  (субъект  $A$ ), так и в  $T_{n2}$  (субъект  $B$ ). Чтобы субъект  $B$  отправил ответ именно в  $T_{n2}$ , то перед ним он помещает в очередь ложное сообщение, тем самым отодвигая отправку истинного сообщения по сети на одну итерацию. Аналогичные ситуации распространяются и на Таблицы 3, 4.

Таким образом, на основе всего вышеописанного, наиболее сильной атакой является сговор внешних и внутренних активных атакующих, при которой необходимым условием противодействия становится либо существование постоянной поточной линии связи, что, в свою очередь, приводит к негации абстрактности и к невозможности применения данной системы в тайных каналах связи, либо принадлежность системы к классу F2F-сетей, что, в свою очередь, приведёт к малым возможностям экспансии.

В результате, если исходить из необходимости синтеза простоты и безопасности системы, то наилучшим вариантом становится выбор F2F-сетей. Это также способно привести к ещё большему упрощению структуры скрытой сети за счёт исключения полиморфизма информации как явления, то есть пункта 3, связанного с маршрутизацией посредством множественного шифрования. Такое действие приведёт к следующим выводам:

1. Исчезнет необходимость в промежуточных узлах и кооперировании с ними для установления периодов. Как следствие, не будет надобности в условностях отправления сообщений на конкретной итерации периода маршрутизирующего узла.
2. Исчезнет необходимость в использовании механизмов несвязываемости размеров сообщений при множественном шифровании [1].
3. Исчезнет необходимость в анализе частного и общего случаев, потому как таковые являются лишь следствием существования маршрутизирующих узлов и полиморфизма информации. И как следствие, пункт 3 заменится пунктом 11<sub>2</sub>.

Вышеописанные действия переводят шестую стадию анонимности на противоречие пятой градации, аналогично первой<sup>^</sup> стадии анонимности. И действительно, если происходит образование анонимной сети на базе пятой стадии анонимности, где перестаёт существовать полиморфизм информации, то подобная система должна будет вбирать основной критерий скрытых сетей, а именно – возможность создавать сервисы связи. Сервисы связи выстроенные в анонимной сети могут быть основаны на второй стадии, что приводит к увеличению  $|T|$  мощности доверия. Это в свою очередь противоречит пятой стадии анонимности по причине её принадлежности к сервисам с теоретически минимальной мощностью доверия. Данный парадокс базируется на специфике запутывающего алгоритма не принадлежащего классу полиморфной маршрутизации. Таким образом, данную стадию нельзя полноценно считать пятой стадией анонимности (по природе своего транслирования информации, а не хранения в роли сервиса связи) и шестой градацией (по причине отсутствия полиморфизма информации). По этой причине и вполне корректно можно считать данный этап пятой<sup>^</sup> стадией анонимности, как это было выявлено и сделано ранее (в работе [1]) с первой<sup>^</sup> стадией анонимности. Этим также доказывается не обязательная принадлежность скрытых сетей к последнему этапу анонимата при первом векторе развития анонимности (ориентированным на безопасность объектов), потому как запутывающим алгоритмом становится «очередь», скрывающая факт истинной передачи информации между субъектами, взамен комбинации «очередь+полиморфизм».

Теоретически основным отличием таковых подходов становятся иные векторы нападения, где при алгоритме «очередь» атаки начинают принадлежать способам

компрометации доверенных узлов, а при алгоритме «очередь+полиморфизм» – компрометациям маршрутизирующих узлов. В обоих случаях требуется сговор скомпрометированного узла с внешним глобальным наблюдателем. При удовлетворении условия нескомпрометированности ключевых субъектов, анонимность двух алгоритмов будет удерживаться на определённо заданном уровне.

Практически же основным отличием доверенной сети от маршрутизирующей становится существование прямой криптографической связи между отправителем и получателем, что приводит к фактически взаимной деанонимизации субъектов, при условии, что один из них становится скомпрометированным узлом. При увеличении участников сети, связанных между собой одной группой, возрастает соответственно и риск деанонимизации. Таким образом, в доверенных системах предполагается, что сами субъекты не защищаются и не скрывают свою идентификацию друг от друга. В то время как маршрутизирующие системы наоборот, с присущим им полиморфизмом информации, предполагают, что все субъекты, включая отправителя или получателя могут быть атакующими, и следовательно, сводят все свои векторы нападения на третью, незаинтересованную сторону.

Поэтому способы применения чистых F2F-сетей (без полиморфизма информации) становятся отличными от других анонимных сетей. Так например, пятую<sup>^</sup> стадию анонимности можно корректно применять лишь при условиях, когда все участники системы способны идентифицировать своих друзей как по сетевому критерию, так и по криптографическому, со знанием их взаимосвязей. Таковой критерий сужает способ применения подобных сетей, т.к. не позволяет применять их в системах, где требуется разграничение анонимности отправителя и получателя между собой.

Помимо прочего, если доверенный узел становится скомпрометированным, то у него появляется возможность узнать, общается ли собеседник ещё с кем-либо в определённый промежуток времени просто отправляя запросы в его сторону. Если по прошествии  $T_n$  времени ответ не был получен, то это говорит о том, что в очереди получателя хранилось как минимум одно сообщение в данный промежуток времени, которое было настоящим запросом или ответом. Подключая внешнего активного глобального атакующего, можно достичь деанонимизации отправителя и получателя, если итеративно блокировать участников и постоянно проверять занята ли очередь. Тем не менее, такая атака может занять очень много времени, если у субъекта уже была загружена очередь сообщений, что в теории может достигать её константного пика, либо если он вставляет случайным образом в очередь «пустые» пакеты, что ещё сильнее может затруднять связность настоящего отправления, либо получения. Также данную проблему можно искоренить внедрением поточного поддержания связи с одним или несколькими субъектами сети, приводящего к взаимоблокировке при отключении, но данное свойство автоматически исключит фактор абстрактности системы.

Также, из-за специфичности очередей, сети такого рода не могут выстраивать сильную концентрацию любых сервисов связи, потому как запрос-ответ со стороны разных субъектов становится единым последовательным действием из-за чего становится невозможным эффективно создавать общий сервис на множество клиентов в один промежуток времени. Как пример, пятая<sup>^</sup> стадия анонимности на базе очередей может эффективно быть применима при построении мессенджеров, с неотслеживаемостью факта переписки (дополнительно с E2E-шифрованием), но не может использоваться при построении файловых-сервисов рассчитанных на множество клиентов. Если существует  $N$ -ое количество субъектов взаимодействующих с файловым-сервисом в один промежуток времени и каждый пытается скачать файл размером в  $X$ , то при размере пакета в  $Y$  (где  $X > Y$ ) с конфигурационным периодом равным  $T_n$  все участники гарантированно смогут скачать

данный файл только спустя  $M = T_n N[X/Y]$ . При увеличении  $N$ , конечная скорость скачивания будет линейно регрессировать, при уменьшении  $T_n$  будет производиться большое количество спама, при котором стабильность работы узлов станет ухудшаться, при увеличении  $Y$  очередь будет содержать меньшее количество объектов для сохранения памяти устройства, тем самым приводя к игнорированию некоторого количества запросов от клиентов. Таким образом, эффективность использования пятой<sup>1</sup> стадии анонимности на базе очередей зависит от конкретных типов задач.

### 3.2. Модель на базе увеличения энтропии

Другой абстрактной анонимной сетью может быть система на базе увеличения энтропии. Со стороны теоретического доказательства анонимности она более трудоёмкая и в некой степени более «хрупкая» (чем сеть на основе очередей), потому как большинство действий сводит к вероятностям конкретно выбранного субъекта, а не к действиям всей группы. Чтобы правильно доказать существование теоретической анонимности в таких условиях – необходимо рассматривать факт связывания субъектов между собой, анализируя при этом постоянный прирост энтропии.

Предположим, что существует всего три узла  $\{A, B, C\}$  и сама сеть работает по принципу вероятностного полиморфизма с множественным шифрованием, где каждый субъект может с вероятностью  $1/2$  выстроить маршрут с промежуточным узлом или без него соответственно. Предполагается, что вся генерируемая информация в такой системе принадлежит монолитному криптографическому протоколу [2] из чего следует, что транспортируемый пакет не хранит в открытом виде идентификацию абонентов. В конечном итоге будет образовано два разных и равновероятно возможных действия.

1. При полиморфизме информации будет существовать три этапа транспортирования информации:  $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$ <sup>1</sup>.

2. При отсутствии полиморфизма информации будет существовать всего два этапа транспортирования информации:  $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$ .

В данном концепте временно предполагается, что системе известен лишь отправитель информации (инициатор), в то время как получатель не определён. Из вышеописанного также следует, что если полиморфизм будет являться статичной величиной (то есть, будет всегда существовать или не существовать вовсе), то определение получателя станет лёгкой задачей, по причине необходимости в генерации обязательного ответа инициатору.

Тем не менее если полиморфизм будет иметь вероятностную величину, то грань между отправлением и получением будет постоянно и постепенно стираться, сливаться, инвертироваться, что приведёт к неоднородному трактованию анализируемых действий: запрос(1) - ответ(1) - запрос(2) может стать равным запросу(1) - маршрутизации(1) - ответу(1). Но в таком случае, возникает свойство гипертелии (сверх окончания), где запрос(2) не получает своего ответа(2), что снова приводит к возможности детерминированного определения субъектов на основании данного анализа.

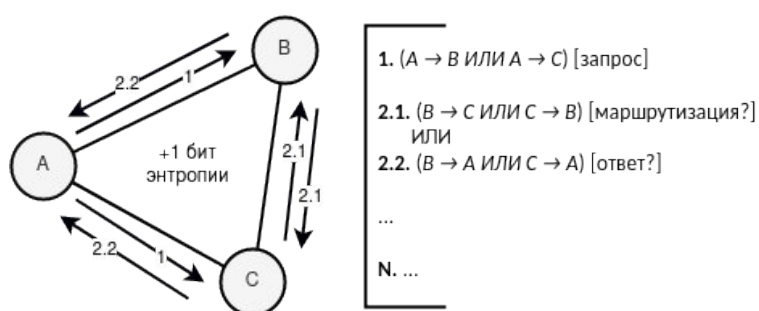
---

<sup>1</sup>Стрелка в скобках указывает отправителя слева и получателя справа, вне скобок стрелка указывает на изменение структуры пакета, сами же скобки предполагают существование одинакового пакета, операция *ИЛИ* указывает вариативность и параллельность отправления.

Теперь, если выровнять количество действий полиморфизма (количество маршрутизации пакета)  $k$  и количество действий без него  $n$  (что представляет собой всегда константу  $n = 2$ ), иными словами придерживаться формулы  $\text{НОД}(k, 2) = 2$ , где  $\text{НОД}$  — наибольший общий делитель, то получим максимальную неопределённость, алеаторность при минимальной константе  $k = 2$ , которую можно свести к следующему набору действий полиморфизма:  $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$ . В итоге все действия начнут трактоваться двумя полностью самодостаточными процессами: запрос(1) - ответ(1) - запрос(2) - ответ(2) или запрос(1) - маршрутизация(1) - маршрутизация(~1) - ответ(1), что в свою очередь приведёт к неопределённости отправления и получения информации со стороны анализа трафика всей сети. И потому, ответ(1) = маршрутизация(1), запрос(2) = маршрутизация(~1), а также ответ(2) = ответ(1) = маршрутизация(2), где последняя добавочная маршрутизация(2) получается из запроса(2). Проблемой, в таком случае, является лишь запрос(1), созданный генезис-инициатором связи, который будет трактоваться всегда детерминировано. Но и здесь, в первую очередь, стоит заметить, что при последующих запросах данная проблема всегда будет угасать из-за увеличивающейся энтропии [4], приводящей к хаотичности действий посредством метаморфозов вероятностного полиморфизма. Так например, на следующем шаге появится неопределённость вида  $\text{запрос}(3) = \text{запрос}(2) = \text{маршрутизация}(\sim 2)$ , означающая неоднозначность выявления отправителя. Итоговую модель можно представить следующим способом:

[illegible]

Таким образом, задача анонимной сети на базе увеличения энтропии формируется сложностью нахождения истинных субъектов информации при трёх и более пользователях не связанных между собой общими целями и интересами для внешнего глобального и внутреннего наблюдателей. Это возможно при использовании слепой маршрутизации в совокупности с вероятностным полиморфизмом пакета, где слепая маршрутизация обеспечивает диффузию пакета, распространяет его и делает каждого узла в сети потенциальным получателем, а вероятностный полиморфизм обеспечивает конфузию пакета, приводит к размытию роли субъектов информации, стирает грань между отправлением и получением. На основе вышеприведённых критериев уже образуется виртуальная маршрутизация, которая скрывает и разрывает связь объекта с его субъектами, приводит к зарождению абстрактной анонимной сети.



**Рисунок 5.** Зарождение неопределённости при вероятностном полиморфизме

При этом, стоит заметить, что в сети на базе увеличения энтропии, на уровне ядра, заложен механизм постоянного умножения, увеличения энтропии, как это представлено на *Рисунке 5*, вследствие чего зарождаются и усваиваются одни лишь ложные логические суждения. Если таковые суждения априори представляют ложные выводы на любые выражения, то это эквивалентно полному доминированию энтропии над системой, в которой становится невозможным выявление закономерностей посредством декомпозиции её составляющих.

Продолжая анализ абстрактной анонимной сети на базе увеличения энтропии, можно выявить, что маршрутизация и ответ в ней, являются этапами полностью автоматизированными, в то время как запрос является этапом ручным. Такой момент приводит к явлению, что между ответом и последующим запросом интервал времени ожидания больше, нежели между запросом - ответом, запросом - маршрутизацией, маршрутизацией - маршрутизацией или маршрутизацией - ответом. Это приводит к возможности осуществления атаки методом учёта времени с последующим расщеплением хаотичности, тем самым приводя к однозначности маршрутизации и к возможному выявлению субъектов информации. Предотвратить подобную уязвимость можно двумя противоположными, дифференциальными и амбивалентными способами:

1. Симуляция времени запроса. Иными словами, маршрутизация и ответ будут подстраиваться под примерное время генерации пакета в сети, способом установления задержки. Чем больше узлов в сети, тем меньше время задержки. Подобный метод следует



использовать только в системах с большим количеством узлов, т.к. с малым количеством время ожидания маршрутизации или ответа будет достаточно долгим.

2. Симуляция времени маршрутизации и ответа. Иными словами, запрос будет подразумевать не только передачу истинной информации, но и передачу ложной, незначимой, пустой информации, в моменты отсутствия настоящего запроса. Подобный метод следует использовать только в системах с малым количеством узлов, т.к. производится огромное количество спама.

Продолжая анализ, можно заметить некоторые закономерности, приводящие к более точному обнаружению состояния пакета при последовательных итерациях запрос - ответ или запрос - маршрутизация - ответ, а именно, является ли он (пакет) запросом или ответом с вероятностью  $\frac{2}{3}$ , что эквивалентно более точному определению состояния субъекта информации.

Исходя из периода  $T$ , который вычисляется по формуле  $\text{НОК}(2+k, 2)$ , где  $\text{НОК}$  — наименьшее общее кратное, несложно узнать, что период при  $k = 2$  будет равен 4. Это в свою очередь говорит о том, что каждое четвёртое действие, начиная с предыдущего запроса, будет с вероятностью  $\frac{2}{3}$  также являться запросом (аналогична ситуация с ответом). Проблема не приводит к выявлению сеанса связи или сессии (потому как данная величина является алеаторной и неопределённой), но при этом делает более транспарентным сам факт существующего отправления/получения. В момент повышения энтропии, когда создаётся коллизия состояний, одновременно зарождается и период, как побочный эффект, противопоставляющий себя непредсказуемости, индетерминированности и дифферентности.

Проблема периода представляет собой лишь более вероятностный способ определения состояния, для решения которой будет достаточным повышение периода двумя возможными способами:

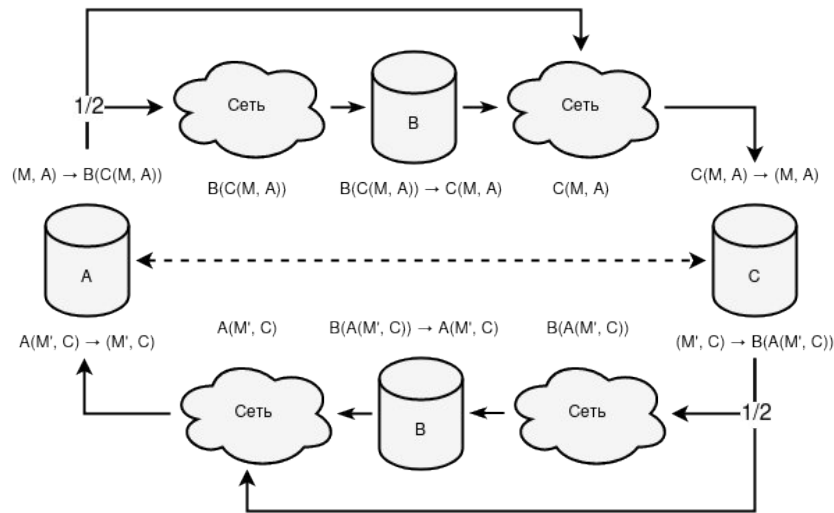
1. Повысить  $k$ . Тогда период  $T = \begin{cases} 2 + k, k \bmod 2 = 0 \\ 2(2 + k), k \bmod 2 \neq 0 \end{cases}$  (не стоит забывать о свойстве гипертелии, если выбор падает на нечётное число).

2. Сделать  $k$  случайной переменной диапазона  $[1;n]$ , где  $n$  — максимальное количество маршрутизаций. Тогда период  $T = \text{НОК}(2, 1+2, 2+2, \dots, n+2)$ .

Далее, если предположить, что существует сговор активного внутреннего наблюдателя и пассивного глобального наблюдателя, то вырисовывается картина неблагоприятная для получателя, т.к. она в конечном счёте будет представлять его деанонимизацию. И правда, если отправитель становится способным формировать собственный маршрут, а также следить за сценарием работы сети посредством знания всех полиморфных состояний своего пакета, то последний узел из списка маршрутизации станет тем, кто выдаст детерминированно ответ на поставленный запрос, и как следствие, самостоятельно создаст изоморфную связь между сетевой и криптографической идентификациями путём выдачи состояния объекта.

Решением должно стать отнесение отправителя ко множеству внешних атакующих, сделать его пассивным анализатором, прослушивателем системы на моменте получения пакета принимающей стороной и последующим транспортированием объекта до иницилирующей стороны. Дополнительное формирование собственных маршрутов на

принимающих узлах может стать частичным или составным решением проблемы, как это изображено на *Рисунке 6*, и привести к полиморфизму вида  $[(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B)] \rightarrow [(B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)]$ , где [] представляет отдельную генерацию маршрутизации пакета. Следовательно, вероятностный полиморфизм станет определением совокупной возможности существования промежуточных субъектов  $\frac{3}{4} = \frac{1}{4}$  (со стороны отправителя) +  $\frac{1}{4}$  (со стороны получателя) +  $\frac{1}{4}$  (со стороны обоих узлов) и их отсутствия  $\frac{1}{4}$ . Таким образом, инициатор связи в конечном счёте станет неспособным со 100% уверенностью определить, что последний узел отправляющий пакет, станет тем самым истинным получателем сообщения.



**Рисунок 6.** Обобщённая схема передачи информации в анонимной сети на базе увеличения энтропии

Но даже в вышеописанном случае остаётся связь при которой получатель должен будет первым формировать всю последующую маршрутизацию, а следовательно и первым, кто будет генерировать новый полиморфный пакет. И т.к. инициатор способен анализировать всю сеть, то выявить субъекта генерирующего пакет отличный от маршрутизирующего первоначально, на первый взгляд, не составит больших проблем. Но данная задача лежит в плоскости долгосрочного наблюдения за субъектами, а не краткосрочного. Проблематика деанонимизации такого случая усложняется алеаторными факторами (каждый промежуточный узел имеет вероятность генерировать псевдо-пакет, симуляция времени маршрутизации и ответа будет постоянно приводить к спаму, получатель способен самолично выставить задержки отклика) порождающими и накапливающими энтропию, которая, как следствие, накладываясь на данную задачу, делает её анализ не таким примитивным и тривиальным — *Рисунок 7*.

Пример предотвращения выявления связи между сетевой и криптографической идентификациями получателя можно представить также на базе метаморфозов вероятностного полиморфизма со стороны иницирующей (атакующей) стороны.

Метаморфозы вероятностного полиморфизма

Расширение энтропии

1.  $(A \rightarrow B \text{ ИЛИ } A \rightarrow C)$   
[# A - инициатор ]  
[# B или C - получатель ]

1. [запрос(1)] →  
| 0 бит |

- |   |   |
|---|---|
| 2. $(B \rightarrow C \text{ ИЛИ } C \rightarrow B) [\# T_{[0;N]}]$<br>$[\# B \text{ или } C - \text{маршрутизатор}]$<br>ИЛИ<br>$(B \rightarrow C \text{ ИЛИ } C \rightarrow B)$<br>$[\# B \text{ или } C - \text{отправитель}]$ | 1. [маршрутизация(1)]<br>=<br>2. [запрос(2)] $\rightarrow$<br>  1 бит |
| 3. $(B \rightarrow A \text{ ИЛИ } C \rightarrow A) [\# T_{[0;N]}]$<br>$[\# B \text{ или } C - \text{получатель}]$   | 3. [ответ(1)] $\rightarrow$<br>  1 бит                                |

В такой концепции свойство задержки  $T_{[0;N]}$  применяется для аккумуляции энтропии. Чем больше участников сети становится, тем больший прирост энтропии способен обеспечиваться в интервале  $T_{[0;N]}$ . При отсутствии данного параметра вероятность нулевого прироста энтропии увеличивается прямо пропорционально уменьшению мощности спама<sup>2</sup> (активности) сети. Таким образом, максимальный диапазон задержки  $N$  должен устанавливаться не меньше среднего времени генерации нового пакета в системе.

Защита от сговора активных внутренних и внешних наблюдателей схожа с анонимной сетью на базе очередей, где становится возможным создание поточной связи с целью взаимоблокировки субъектов, либо создание доверенных соединений с целью установки сложности встраивания в сеть зловердных узлов.

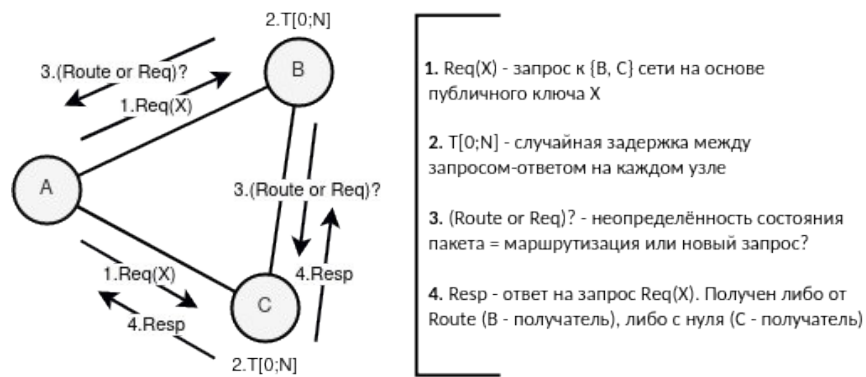
<sup>2</sup>Мощность спама — количество сгенерированных уникальных пакетов в системе за определённый период времени  $t$  совершённый разнородными (никак не связанными между собой общими целями и интересами) участниками сети. Из данного определения следует, что мощность спама не может превышать количество её участников ни в какой выбранный промежуток времени, потому как два и более сгенерированных пакета одним пользователем будут считаться за один, по причине однородности узла к самому себе. Уровень заспамленности становится в некой мере ключевым фактором безопасности большинства анонимных сетей, т.к. «размывает» связь между истинными субъектами посредством перемешивания множества объектов в сети.

$$|S_t| = \sum_{i=1}^{|L|} F(\sum_{j=1}^{|L_i|} ((F * G)(t \bmod P(L_{ij}))))$$

где  $F: N \cup \{0\} \rightarrow \{0, 1\} = \lfloor x / (1+x) \rfloor \Rightarrow 0 \rightarrow 0; x \neq 0 \rightarrow 1,$   
 $G: \{0, 1\} \rightarrow \{0, 1\} = x + 1 \pmod{2} \Rightarrow 0 \rightarrow 1; 1 \rightarrow 0,$   
 $L = Q(M),$   
 $M$  – множество всех узлов в сети,  
 $Q$  – функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами,  
 $P$  – период генерации пакета на базе выбранного узла.

Если  $t$  представлено как НОК от всех  $P(L_{ij}) \rightarrow \text{НОК}(P(L_{11}), P(L_{12}), \dots, P(L_{21}), P(L_{22}), \dots, P(L_{nm}))$ , то в заданный промежуток времени мощность спама обретает своё максимальное значение  $|S_t| = |L|$ . Примером может служить таблица вычисления мощности спама при  $L = \{A, B\}, \{C\}, \{D\}$ ,  $P(A) = 1, P(B) = 2, P(C) = 3, P(D) = 2$ , где  $\text{НОК}(P(A), P(B), P(C), P(D)) = 6$ .

	$t_1$	$t_2$	$t_3$	$t_4$	$t_5$	$t_6$
$A$	+	+	+	+	+	+
$B$	-	+	-	+	-	+
$C$	-	-	+	-	-	+
$D$	-	+	-	+	-	+
	$ S_t  = 1$	$ S_t  = 2$	$ S_t  = 2$	$ S_t  = 2$	$ S_t  = 1$	$ S_t  = 3$



**Рисунок 7.** Неопределённость выявления получателя при атаке сопоставления связей между сетевой и криптографической идентификациями на инициирующей стороне

Принципиальное отличие сети на базе очередей, от увеличивающей энтропию, сводится к способу сдерживания мощности спама. В первом случае мощность спама разбивается по периодам (очередям) заданным самой системой, а потому и активность становится статичной, постоянной и определяемой величиной. Если периоды генерации будут сильно различаться между собой, то начнётся образование новых и дополнительных векторов нападения на систему. Во втором случае сдерживание мощности спама становится следствием алеаторного характера функционирования сети, удерживающего анализ поведения субъектов на базе накапливающейся меры неопределённости – энтропии. Таким образом периоды  $T_n$  и  $T_{[0;N]}$  являются родственными явлениями объединёнными принципом мощности спама.

В сравнении с абстрактной анонимной сетью на базе очередей, сеть на базе увеличения энтропии имеет свои положительные стороны. Во-первых, нет необходимости в ожидании очередей, что приводит к относительно быстрым откликам субъектов информации за счёт возможности параллельных действий. Во-вторых, из-за данного аспекта сеть на базе очередей становится неэффективной в удержании сервисов связи, потому как таковым жизненно необходимо иметь свойство параллельности. Тем самым, сети на базе очередей работают наиболее эффективно лишь и только в полностью децентрализованных системах, гибридность напротив будет приводить к большим задержкам отклика, что нельзя сказать о сетях на базе увеличения энтропии.

Отрицательными характеристиками сети на базе увеличения энтропии, в сравнении с сетью на базе очередей, являются необходимость в полиморфной маршрутизации (в том числе и при доверенных соединениях), а также необходимость в контроле накапливания энтропии. Данные случаи могут достаточно сильно усложнять систему и приводить к неправильным программным реализациям.

### 3.3. Модель на базе обедающих криптографов

Ещё одну из множества возможных моделей можно построить на базе существующих скрытых систем вида DC-сетей, с присущей им теоретически доказуемой анонимностью. По умолчанию сети на базе «проблемы обедающих криптографов» не являются абстрактными, потому как привязаны к своей сетевой топологии типа «полносвязная». В такой архитектуре исключается возможность вариативного расположения узлов по всему множеству сетевых коммуникаций. Допустим, в чистом виде DC-сети нельзя применять так, чтобы вычисление результата проходило только через одного участника, потому как таковой в последствии

будет способен деанонимизировать всех остальных субъектов и переведёт анонимную сеть в этап второй стадии анонимности.

Возможным решением перевода DC-сетей в модель абстрактности становится использование комбинации первой<sup>^</sup> стадии анонимности с пятой, посредством которой информация сможет распространяться по сети без увеличения мощности доверия. В такой системе сетевая идентификация окончательно заменяется криптографическим аналогом, а композиция приобретает вид «пятая стадия анонимности + первая<sup>^</sup> стадия анонимности + тайный канал связи». Комбинация «первая<sup>^</sup> стадия анонимности + тайный канал связи» является классическим определением анонимной сети на базе DC-сетей, необходимое для ограничения получателей информации в широкополосной линии связи. Прибавочная «пятая стадия анонимности» становится следствием в необходимости иного распространения информации по широкополосной линии связи, таким образом, чтобы промежуточный субъект легко мог транслировать и маршрутизировать поступающие ему пакеты, но не мог их читать в открытом виде или редактировать содержание.

Таким образом, заменив сетевой способ широкополосной связи на криптографический, становится возможным использование абстрактных DC-сетей в качестве второй формы тайных каналов связи. Также, плюсом такого подхода композиций, с заранее существующими скрытыми сетями и их преобразованием в абстрактные сети, становится наследственность в доказуемости уровня анонимности. Иными словами, если анонимная сеть до преобразования в абстрактную являлась теоретически доказуемой, то и после такого изменения она в равной степени останется теоретически доказуемой, потому как сам внутренний механизм функционирования не изменится, изменится лишь внешний способ идентификации субъектов между собой.

## 4. Заключение

Абстрактные анонимные сети представляют собой достаточно большой интерес для последующих исследований, потому как позволяют поддерживать теоретически доказуемую анонимность в уже существующих, подконтрольных централизованных системах. В сравнении с другими анонимными сетями, абстрактные сети наиболее эффективно разделяют сетевые и криптографические коммуникации за счёт чего становится неважным факт существования «цепочек» маршрутизаций для сохранения анонимата субъектов. С другой стороны, на базе приведённых моделей абстрактных анонимных сетей, проблемой таковых систем становится свойство масштабируемости, которое не позволяет принимать большое количество соединений. Таким образом, абстрактные анонимные сети становятся способными обеспечивать анонимизацию трафика лишь для малого круга лиц.

## Список литературы

1. Коваленко, Г. Теория строения скрытых систем [Электронный ресурс]. — Режим доступа: [https://github.com/number571/go-peer/blob/master/docs/theory\\_of\\_the\\_structure\\_of\\_hidden\\_systems.pdf](https://github.com/number571/go-peer/blob/master/docs/theory_of_the_structure_of_hidden_systems.pdf) (дата обращения: 04.01.2023).
2. Коваленко, Г. Монолитный криптографический протокол [Электронный ресурс]. — Режим доступа: [https://github.com/number571/go-peer/blob/master/docs/monolithic\\_cryptographic\\_protocol.pdf](https://github.com/number571/go-peer/blob/master/docs/monolithic_cryptographic_protocol.pdf) (дата обращения: 04.01.2023).

3. Popescu, B., Crispo, B., Tanenbaum, A. Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System [Электронный ресурс]. — Режим доступа: <http://turtle-p2p.sourceforge.net/turtleinitial.pdf> (дата обращения: 29.12.2021).
4. Шеннон, К. Теория связи в секретных системах [Электронный ресурс]. — Режим доступа: <https://web.archive.org/web/20141222030352/http://pv.bstu.ru/crypto/shannon.pdf> (дата обращения: 02.01.2022).