Теория строения скрытых систем

Коваленко Геннадий Александрович

1. Введение

Централизация существующих систем представляет собой закономерно историческое развитие Интернет коммуникаций в целом. Эволюция первичной децентрализации неизбежно приводит к своему постепенному и логическому отмиранию, к постоянному поглощению и пожиранию централизацией, к концентрации линий связи, к монополии соединений. Централизация, представляя свои отрицательные характеристики, приводит одновременно и к безусловным преимуществам, противоречиво ставших для нас стагнацией дальнейшего развития сетевых взаимодействий. Комфорт, простота использования и лёгкость поддержки приводят к значительным рискам компрометации личной, профессиональной или секретной информации. Скрывая, но не защищая, система манипулирует общественным сознанием, создавая иллюзию уже существующей безопасности и параллельно её незначимости, акцидентальности и даже обсценности.

Таков театр безопасности преследует одновременно две цели, как экономическую, так и политическую. Базовый интересов - это безусловно искусство продать рекламу, сделать так, чтобы «релевантность» запросов постоянно преследовала конечных покупателей, достигала их и покоряла «альтруизмом» маркетологов. Прибыль как цель - такова основная суть современной централизации. Политические интересы - это продолжение экономических, где давление и поглощение какой бы то ни было конкуренции, оппозиции и сопротивления является способом сдерживания и удерживания уже устоявшихся основоположений. Таким образом, обобщая две цели можно заметить их связь, где в одном случае экономическая составляющая играет роль распространения информации, а в другом, политическая основа сдерживает распространение информации для иных (децентрализованно безопасных, как неконтролируемых средств распросранения информации) и схожих участников ролевой модели (централизованных конкурентов, как соперников маркетинга и прибыли). Любое возрождение децентрализации, в идее которой лежит безопасность пользователей, является априори враждебной и приводящей к дальнейшему её подавлению, вплоть до скорейшего уничтожения. Связано это с тем, что в отличие от централизованных конкурентов, никак не разрушающих устоявшуюся систему, децентрализованная система представляет значимую опасность и угрозу, т.к. приводит к умервщлению корневищ, к созиданию ризоморфных состояний.

Дальнейшее развитие сетей разумно предлагает отрицание централизации из-за внутренних противоречий, постепенно пожирающих её изнутри. Отрицание централизации приводит к децентрализации, как более совершенной форме, в отличие от её первичного олицетворения, служащего лишь инициализацией сетевого базиса. Развитие одноранговых систем прокладывает путь через гибридность централизации с децентрализацией, через их объединение и противостояние. Единство положительных сторон централизации, как комфорт использования и лёгкость поддержания, и децентрализации, как отказоустойчивость и безопасность конечных пользователей, является мощным и одновременно сложным сочетанием, которое приводит постепенно к внутренним противоречиям. Комфорт заканчивается там, где начинается усиленное продвижение безопасности, безопасность там, где комфорт становится лидирующей концепцией, отказоустойчивость завершается там, где возникает потребность в

простоте воспроизводства, доступность к систематизации там, где наступает нужда в хаотичности.

Для решения подобных противоречий должен существовать только один фундамент, на котором уже будут располагаться соединения. Централизованные сети возводят удобство на первый план, а безопасность делают акцидентальным критерием, децентрализованные же сети напротив, ведут к основоположению безопасности, возлагая удобство в качестве придатка. Всё вышеописанное есть борьба противоположностей, приводящая в одном случае к регрессу, в другом к прогрессу, и само движение направления зависит от силы общественного сознания, от построенных им, или для них, приоритетов.

2. Первичная проблематика

При рассмотрении вопросов, базируемых на безопасности каналов связи, использующих криптографические протоколы с участниками *A* и *B*, а также с доверенным участником *T*, концентрация внимания сосредоточена в большей мере как раз на последнего. Это логично, ведь доверенный, промежуточный субъект информации *T* становится законно установленным атакующим первоначальными субъектами *A* и *B*, способным совершать MITM атаки (man in the middle) и переводящим систему в неустойчивое состояние, состояние требующее абсолютного доверия. Приведённая атака ссылается на нерешённую проблему доверия[1], разрушительную и губительную по своей сути, но при этом затмевающую более скрытую и деструктивную, мощь которой в современном мире превосходит прямолинейные MITM атаки. Целью нашей статьи служит выявление данного метода нападения, его анализ и последующие решения.

Сутью проблемы является возможность атаки со стороны принимающей стороны, возникающая на фоне криптографических протоколов адаптируемых под защиту связи клиент-сервер, где сервер выдвигается как получатель информации, а клиент как отправитель. При этом, в большинстве случаев сервер вовсе не является настоящим получателем, а представляет собой лишь промежуточный, интерстициальный узел, целью которого служит связывание двух и более клиентов между собой, образуя тем самым новый тип связи клиент-клиент, который в свою очередь криптографические протоколы игнорируют совсем. Такая проблема критична в самом базисе компьютерных сетей, т.к. выдаёт всю информацию субъектов (интересы, сообщения, контактную информацию, политические взгляды и т.д.) в предельно открытом, прозрачном, транспарентном состоянии субъекту-посреднику. Примером такого явления служат современные мессенджеры, социальные сети, форумы, чаты, файловые сервисы и т.д., где общение не происходит напрямую (как это предполагается в криптографических протоколах), а всегда проходит сквозь стороннюю точку, представляющую собой сервис или платформу связи.

Описанное явление начинает претерпевать кардинальные изменения, т.к. возвращает фундаментальную проблему и задачу классической криптографии — борьбу с прослушиванием, которая должна была решиться (и решилась теоретически) лишь с приходом раздела асимметричной криптографии [1]. Данная апория куда серьёзнее и значимее, нежели классическая MITM атака и требует куда меньшее количество затрат атакующего для слежки большего

[1] Проблема доверия — невозможность построения безопасной, монолитной и саморасширяющейся системы, основанной полностью на криптографических алгоритмах для конечных субъектов, без использования промежуточных узлов, удостоверяющих идентификацию абонентов, либо без сторонних каналов связи с заранее установленным доверием. Задача возникает на фоне сложности передачи публичных ключей. В децентрализованных, ризоморфных системах данная проблема куда более значима, т.к. оставляет лишь метод использования сторонних каналов связи, то-есть прямого доверия, через которое уже может образовываться сеть доверия.

количества атакуемых. Это есть паноптикум современного общества, где атакующие и атакуемые меняются местами, инвертируют способ слежения и делают заложника инициатором собственного подслушивания. Теперь жертвы самостоятельно подключаются к заведомо прослушиваемой связи, выбирают множество возможных опций слежения за собственным «Я», в то время как атакующие лишь создают аналогичные соединения, воспроизводят платформы слежения в таком необходимом количестве, чтобы затмевать своим присутствием сам факт существования более защищённых альтернатив. Таким образом, с одной стороны конфиденциальность современных сервисов становится лишь декорацией, театром безопасности, симулякром ссылающимся на несуществующую, гипостазированную безопасность, как на магическое слово маркетинга, оболочку воображаемого величия, а с другой стороны само удобство сервисов начинает быть фундаментом, мыслью, философией, пропагандой противопоставляющей себя безопасности, конкурирующей с ней, постепенно и незаметно заменяющей её, как «Cymothoa exigua».

Итогом такого развития считается возникновение систем доверия, где не только сами доверительные узлы являются атакующими, но и промежуточные получатели, что приводит к значительным и значимым рискам компрометации хранимых и передаваемых объектов между истинными субъектами. Безоговорочно уничтожить такую систему доверия не представляется возможным из-за появления более общих и разрушительных видов атак, ухудшения оптимизации и производительности программ, а также невозможности полного искоренения доверия как такового [2, с.267]. Таким образом, остаётся лишь улучшать данную систему, делать так, чтобы сам её механизм стремился к уменьшению мощности доверия[2], чтобы собственная её структура представляла защиту объектов и анонимат субъектов. К системам подобного рода относятся анонимные сети и тайные каналы связи.

3. Анонимные сети

Скрытые, тёмные, анонимные сети – есть сети, грамотно соединяющие и объединяющие маршрутизацию вместе с шифрованием. Маршрутизация обеспечивает критерий анонимности, направленный на субъект, шифрование – критерии конфиденциальности, целостности, аутентификации, направленные на объект. Без маршрутизации легко определяются отправитель/получатель, без шифрования легко определяется передаваемое сообщение. Таким образом, только в совокупности этих двух свойств сеть может являться скрытой.

В современном мире большинство скрытых сетей представляют оверлейные соединения, иными словами соединения, которые основаны на уже существующей сети (например, сети Интернет). Но так или иначе, это не говорит, что скрытые сети не могут существовать сами по себе и быть однородной структурой, т.к. первоначальная архитектура может быть изначально нацелена на анонимность и безопасность, как например, это описано в проекте NETSUKUKU. Именно по историческим причинам, современные сети имеют оверлейные уровни безопасности.

---

[2] Мощность доверия — количество узлов, участвующих в хранении или передаче информации, представленной дли них в открытом представлении. Иными словами, такие узлы способны читать, подменять и видоизменять информацию, т.к. для них она находится в предельно чистом, прозрачном, транспарентном состоянии. Чем больше мощность доверия, тем выше предполагаемый шанс компрометации отдельных узлов, а следовательно, и хранимой на них информации. Принято считать одним из узлов получателя. Таким образом, нулевая мощность доверия будет возникать лишь в моменты отсутствия каких-либо связей и соединений. Если мощность доверия равна единице, это говорит о том, что связь защищена, иными словами, никто кроме отправителя и получателя информацией не владеют. Во всех других случаях мощность доверия будет больше единицы, что говорит о групповой связи (то-есть, о существовании нескольких получателей), либо о промежуточных узлах, способных читать информацию в открытом виде.

Любая анонимная сеть основывается либо на одноранговой, либо на гибридной архитектуре сети, исключая при этом многоранговую. Многоранговая сеть (или клиент-серверная архитектура) не может быть достаточно анонимной априори, потому как имеет открытую, прямую видимость и непосредственную реальность централизации. Централизация со стороны компьютерных сетей примитивна, но централизация со стороны скрытых сетей не так очевидна. В компьютерных сетях под централизацией понимается ограниченное количество серверов, способных обслуживать куда большее количество клиентов. Когда же говорим об анонимных сетях, то централизация в таких системах может иметь свойство приходящее и уходящее, тем самым, измеряя уровень централизации не в виде булевой логики, а в виде процентных соотношений от всей суммарности сети.

В одноранговых системах все пользователи однородны, имеют одинаковые возможности, могут представлять одни и те же услуги маршрутизации. Такие сети легко могут разворачиваться в локальных системах, но с осложнениями работают в глобальном пространстве на основе уже созданных соединений. Сами одноранговые сети могут быть разделены на две категории: децентрализованные и распределённые, хоть их различие и туманно со стороны терминологии. Распределённые сети можно именовать «истинно децентрализованными», где нельзя выделить какой-либо центр или узел связи сразу нескольких других узлов. Характерной чертой такой сети является тот факт, что каждый пользователь одновременно соединяется напрямую со всеми другими узлами. Децентрализованные же сети можно именовать «слабо централизованными», где к одним узлам сети подключаются сразу несколько других узлов. Характерной чертой такой сети является тот факт, что появляются «неофициальные» узлы, часто используемые другими узлами (узлы-серверы) в качестве последующей маршрутизации.

Гибридная система объединяет свойства многоранговых и одноранговых архитектур, пытаясь взять и удержать как можно больше положительных и меньше отрицательных качеств. Плюсом многоранговых архитектур являются некоторые свойства централизации, как например возможность разделения логики на серверную и клиентскую, более быстрая и/или статичная скорость маршрутизации. Плюсом одноранговых архитектур являются некоторые свойства децентрализации, как собственно возможность достижения и построения анонимности. Гибридные сети не всегда можно однозначно определить, иногда они выглядят и/или ведут себя сродни одноранговым, иными словами, используют минимальное количество свойств многоранговой архитектуры, или наоборот, могут иметь вид многоранговой архитектуры и даже перерастать в неё полностью. Из всего этого многообразия, гибридные сети являются самой противоречивой системой.

Анонимность также не является чем-то однородным, точно определённым, её можно трактовать как некую градацию, поэтапность, которой присуще шесть стадий, выявляющих процесс её формирования.

1. Первая стадия является исходной точкой анонимности, тезисом, монадой не представляющей анонимность, пустотой инициализирующей мощность анонимности[3] $|A|$

[3] Мощность анонимности — количество узлов, выстроенных в цепочку и участвующих в маршрутизации информации от отправителя до получателя, при этом, не будучи никак связанными между собой общими целями и интересами. Из этого следует, что многоранговая архитектура по умолчанию имеет мощность анонимности равной единице (вне зависимости от количества серверов). Нулевая мощность анонимности возникает либо при отсутствии связей, либо при существовании прямого соединения между субъектами (иными словами при отсутствии какой бы то ни было маршрутизации).

$$|A| = |F(N)| - \sum_{i=1}^{W} \begin{cases} 0, W_i = \varnothing \\ |W_i| - 1, W_i \neq \varnothing \end{cases},$$

$= 0$. Примером является отсутствие связи как таковой или существование только прямого, прямолинейного, примитивного соединения между двумя одноранговыми субъектами, что равносильно их стазисному состоянию.

2. Вторая стадия, становясь антитезисом, начинает отрицать первый этап, приводить систему к первичному метастасизу, изменять собственным преобразованием способ взаимодействия между субъектами, добавлять к своей оболочке новую роль промежуточного узла, сервера, подчиняющего всех остальных субъектов к частно-личному сервису. Таким образом, архитектура становится многоранговой, клиенты начинают зависеть от платформ связи, а мощность анонимности повышается до константного значения. Этап обеспечивает только анонимность клиент-клиент, но игнорирует при этом анонимность клиент-сервер, что и приводит к статичной мощности анонимности $|A| = 1$. Иными словами, сервер начинает обладать достаточной информацией о клиентах, клиенты в свою очередь начинают коммуницировать под средством сервера, что приводит их к фактическому разграничению, к взаимной анонимности под средством общей платформы. Стоит также заметить, что анонимность и безопасность здесь идут вразрез друг с другом, противопоставляют себя друг другу, где с одной стороны безопасность связи клиент-клиент становится скомпрометированной и дискредитированной, в то время как с другой стороны анонимность связи клиент-клиент является инициализирующей и первой простейшей формой анонимата. Такое противоречие (ухудшения безопасности и улучшения анонимности) не является случайным, а представляет собой правило и закономерность, в чём можно будет ещё убедиться. Описанную стадию вкратце именуют псевдо-анонимностью, а клиентов — анонимами.

3. Третья стадия представляет примитивную маршрутизацию, а следовательно и примитивную анонимность, нескольких прокси-серверов несвязанных между собой. Именно на данном этапе сеть становится раздробленной, неопределённой, гибридной за счёт чего и повышается мощность анонимности либо статичным $|A| \approx N$, либо динамичным способом $0 < |A| \leq N$, где N - количество прокси-серверов. Первый метод предполагает выстраивание цепочки узлов, через которые будет проходить пакет. в то время как второй способ представляет собой слепую, заливочную маршрутизацию от одного ко всем [3, с.398]. Мощность анонимности на данном этапе действительно повышается, но безопасность самих субъектов ещё никак не обеспечивается. Связано это всё потому, что шифрование на данном этапе есть свойство добавочное (сродни второй стадии), не обеспечивающее защиту связи клиент-клиент, а следовательно, и не приводящее к уменьшению мощности доверия.

4. Четвёртая стадия, являясь синтезом предыдущих стадий, становится и точкой окончательной замены сетевого адреса криптографическим, при которой идентификация субъектов отделяется от концепции сетевых протоколов, подчиняя узлов абстрактно криптографической модели. Строятся платформы сетевой связи как базисы, поверх которых разрастаются криптографические соединения, инкапсулируя тем самым взаимодействия субъектов от своего основания. Именно на данном этапе мощность доверия становится минимально возможной величиной, а потому и все приложения построенные

где $W = E(F(N))$, N - множество узлов, расположенных в сети,
F - функция выборки множества узлов, участвующих в маршрутизации,
E - функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами.

на четвёртой стадии анонимности, имеют уровень безопасности зависимый только (или в большей мере) от качества самой клиентской части. Примером такой стадии могут являться чаты, мессенджеры (Bitmessage), электронная почта, форумы (RetroShare), файловые сервисы (Freenet, Filetopia), блокчейн платформы (Bitcoin, Ethereum) [4] и т.д., где главным фактором идентификации клиентов являются криптографические адреса (публичные ключи, хеши публичных ключей). Сеть представляет собой также, как и в третьей стадии, гибридный, разрозненный характер поведения узлов вместе с тождественностью мощности анонимности. Четвёртую стадию можно охарактеризовать игнорированием анонимности (экзотеричностью) со стороны субъекта и её сохранением (эзотеричностью) в передаваемом объекте.

5. Пятая стадия приводит к отрицанию четвёртой стадии, как системы не ориентированной на анонимность, изменяет способ маршрутизации, придавая ему свойство полиморфизма, изменчивости закрытой информации по мере перехода от одного узла к другому, отстраняя при этом самих узлов к анализу и сравниванию шифрованной информации. Таким методом скрывается настоящая связь между субъектами под средством их объекта, а следовательно и анонимат обретает истинный характер, при котором сама система начинает стремиться к увеличению и сдерживанию мощности анонимности — $lim_{|A|\to C}$, где C - количество узлов участвующих в маршрутизации. Примером пятой стадии является большинство скрытых сетей, подобия Tor (onion routing), I2P (garlic routing), Mixminion (mix network) и т.д.

6. Шестая стадия повышает анонимность до абсолюта, теоретического максимума за счёт объединения свойств полиморфной и слепой маршрутизации, образовывая новую, вероятностную (виртуальную) маршрутизацию. Данный этап применяет конъюнкцию на основные характеристики четвёртой и пятой стадий, иными словами, предполагает распространение объекта по всем узлам с вероятностной возможностью его полиморфизма. Мощность анонимности определяется следующим методом — $lim_{|A|'\to C} \leq |A| \leq N$, где N - количество узлов в сети, C - количество узлов участвующих в маршрутизации из всего множества сети. Двойственная мощность, с неравенством и пределом, обуславливается двойным способом маршрутизации. Данный этап может быть основой, ядром скрытых сетей, а также тайных каналов связи. В отличие от пятой стадии анонимности, где скрытые сети могут быть как одноранговыми, так и гибридными, сеть на основе шестой стадии может быть только одноранговой.

Стоит заметить, что шифрование, определяемое анонимностью, появляется частично лишь в моменты четвёртой стадии, в то время как на второй и третьей стадиях само шифрование является добавочным, дополнительным, акцидентальным свойством, служащим лишь и только для защиты клиент-серверной коммуникации.

Основным моментом четвёртой стадии является возможность идентификации субъектов в одноранговых и гибридных системах, что ведёт к целостности, а также и к аутентификации самой передаваемой информации, не зависимой от сторонних узлов и серверов [5, с.223]. Помимо прочего, может также и появляться свойство конфиденциальности, где информация представляет собой суть секретного, скрытого, тайного, а не открытого и общего объекта. Но данного свойства может и не быть на четвёртом этапе, если оно является избыточным для самой системы. Как пример, в криптовалютах имеются свойства целостности и аутентификации, но не конфиденциальности. Только начиная с пятой стадии анонимности, конфиденциальность становится базисом системы.

Большинство атак, направленных на скрытые сети, представляют способы деанонимизации субъектов (как наиболее лёгкий способ), нежели попытки раскрытия, взлома, дешифрования объектов (как наиболее сложный). Так, например, достаточно сильной и сложно искоренимой атакой на одноранговые (а следовательно, и на гибридные) сети является атака Сивиллы. Она базируется на том факте, что главным способом анонимности является элемент маршрутизации, который обеспечивается за счёт передачи информации посредством нескольких узлов. С одной стороны, сутью атаки является замена несвязанных между собой узлов, на узлы подчинённые одному лицу, либо группе лиц с общими интересами, тем самым, атака ориентируется на ($lim_{|A|\to 1}$) уменьшение мощности анонимности до единицы. С другой стороны, в некоторых видах сетей с увеличенной мощностью доверия, атака может вредить и целостности передаваемой информации, иными словами, подменять и видоизменять её. При повышении количества узлов несвязанных между собой в сети, повышается и сложность реализации атаки Сивиллы, за счёт более равномерного распределения узлов. Из этого также следует, что мощность анонимности будет стремиться к своим теоретически заданным значениям. Всё это связано с тем, что атакующие узлы будут конкурировать с обычными узлами за возможность быть посредниками между субъектами передаваемой информации. Чем больше несвязанных узлов и лучше алгоритм распределения, тем меньше вероятность осуществления данной атаки. Тем не менее атака Сивиллы особо опасна при этапе зарождения скрытых сетей, когда количество узлов минимально. Решений данной проблемы несколько:

1. Обеспечить замкнутость и сложность встраивания узлов в сеть. Иными словами, использовать фактор доверия или параметр дружбы. Узлы в таких сетях должны выстраивать связи между собой, основываясь на субъективности к уровню доверия, т.к. никакого объективно доверенного, а следовательно, и централизованного, узла не существует. Выстраивая связи друг-к-другу (или friend-to-friend), узлы также начинают выстраивать связи друг моего друга — это мой скрытый друг. Таким образом, друзья друзей не подключаются напрямую и не знают друг друга, но при этом вполне могут обмениваться информацией между собой, что является показателем увеличения размеров сети. Чтобы успешно подключиться к такой сети, необходимо самому стать доверенным узлом, то-есть пользователем, которому кто-либо доверяет. Сложность исполнения атаки, на такой род сети, сводится к сложности встраивания в сеть подчиняемых узлов, как того требует атака Сивиллы, а это, как было описано выше, является проблематичным действием. Единственная проблема friend-to-friend (f2f) сетей заключается в их малой эксплозии, расширении, увеличении масштаба, являясь тем самым следствием причины ручной настройки и установки списка доверенных узлов.

2. Осуществить переход к шестой стадии — крайней форме анонимности. В таком случае, целью является сокрытие, удаление, исключение всех возможных связей между отправляемой информацией (объектом) и самим отправителем/получателем (субъектом). После исчезновения всех связей, сама маршрутизация перестаёт быть чем-то реальным и настоящим перерастая тем самым в этап условного и виртуального, где раскрытие даже одного из субъектов, начинает быть сложной задачей. Деанонимизация в таком случае возможна лишь при условии полного внутреннего контроля сети, по причине сложного обнаружения и последующего восстановления связей с объектом. Основным и главным отрицательным свойством шестой стадии анонимности является линейное увеличение нагрузки на сеть *O(N)* со стороны всех пользователей в ней участвующих. Так, например, если сеть состоит из *N* узлов, то каждый узел должен будет обрабатывать *N-1* запросов от других узлов. Время жизни пакета (TTL) на шестой стадии не является решением данной

проблемы, по причине появления новых связей между отправителем и передаваемой информацией, что, следовательно, приводит к деструкции базиса, к дисфункции сокрытия связей, к деградации виртуальной маршрутизации, и как итог, к переходу на пятую стадию анонимности.

Атака Сивиллы может быть рассмотрена и более обще, где вместо встраивания узлов в скрытую сеть, происходит образование первичной сети, на основе которой будет существовать последующая тёмная сеть. Такой вид атаки может существовать лишь при оверлейных соединениях, коим и является сеть Интернет. Если вся тёмная сеть будет воссоздана в первичной сети, подконтрольной одному лицу или группе лиц с общими интересами, то, следовательно, и весь трафик скрытой сети возможно будет анализировать, с момента её появления и до момента её гибели. Подобная атака требует огромных ресурсов и первоначально настроенной инфраструктуры, что в современных реалиях под силу лишь государствам. Предотвратить такой вид атаки крайне сложно, но вполне возможно, если соблюдать два правила:

1. Использовать противоречия государств — вариативные и несогласованные законы, политические и империалистические интересы. Всё это есть моменты, при которых одно государство не будет выдавать информацию о своей сети другому государству. И чем более агрессивно настроены страны по отношению друг к другу, тем менее успешно они могут контролировать свои собственные ресурсы. В таком случае, необходимо строить сеть по федеративному принципу, чтобы узлы располагались на разных континентах мира, странах и государствах.

2. Использовать изменения информации в процессе её маршрутизации. При таком способе информация будет представлена в полиморфной и самоизменяющийся оболочке, то-есть оболочке шифрованной. Такой подход необходим в моменты, когда информация, приходящая из государства A в государство B, будет снова возвращаться на свою родину A[4]. В качестве примера можно привести луковую маршрутизацию сети Tor, где само шифрование представлено в виде слоёв, которые каждый раз «сдирают», снимают при передаче от одного узла к другому.

Существует также и альтернативный вариант противодействия подобной атаке. Он в отличие от вышеописанного не требует этапа с федеративностью, но взамен требует огромное количество информации, приводящую к спаму. Плюсом такого подхода является и то, что его можно использовать в тайных каналах связи как единственно возможный элемент анонимизации субъектов. Для осуществления такого метода применяются сети основанные на шестой стадии анонимности, т.к. они распространяют информацию методом заливки, что априори ведёт к множественному дублированию, пролиферации. Полиморфизм информации осуществляется способом установки промежуточных получателей (маршрутизаторов) и созданием транспортировочных пакетов, представленных в форме множественного шифрования. Как только узел сети принимает пакет, он начинает его расшифровывать. Если пакет успешно расшифровывается, но при этом сама расшифрованная версия является шифрованным экземпляром, то это говорит о том, что данный принимающий узел — это промежуточный получатель, целью которого является последующее распространение «расшифрованной» версии

[4] Мощность федеративности — количество государств, не связанных общей военной силой, через территорию которых проходит маршрутизация полиморфной информации. Из этого следует, что если сеть разворачивается лишь в пределах одного государства, то мощность федеративности по умолчанию будет равна единице. Нулевой мощности федеративности не существует.

пакета по сети. Рекуперация, в совокупности с конечной рекурсией, будет происходить до тех пор, пока не будет расшифрован последний пакет, предполагающий существование истинного получателя, либо до тех пор, пока пакет не распространится по всей сети и не окажется забытым, по причине отсутствия получателя (будь то истинного или промежуточного). Стоит также заметить, что маршрутизаторы при расшифровании пакета могут узнавать криптографический адрес отправителя, именно поэтому стоит отправлять транспортировочные пакеты из-под криптографического псевдо-адреса отправителя.

Пример программного кода [6] для создания транспортировочного пакета:

```
import (
	"bytes"
)
func RoutePackage(sender *PrivateKey, receiver *PublicKey, data []byte, route []*PublicKey) *Package {
	var (
		rpack  = Encrypt(sender, receiver, data)
		psender = GenerateKey(N)
	)
	for _, pub := range route {
		rpack = Encrypt(
			psender,
			pub,
			bytes.Join(
				[][]byte{
					ROUTE_MODE,
					SerializePackage(rpack),
				},
				[]byte{},
			),
		)
	}
	return rpack
}
```

Если предположить, что в сети существует всего три узла {*A, B, C*} (где один из них является отправителем — *A*) и сама сеть основывается на шестой стадии анонимности без полиморфизма информации, то в таком случае и при таком условии крайне проблематично определить истинного получателя, пока он сам себя не выдаст ответом на запрос (т.к. ответом будет являться совершенно новый пакет, отличный от всех остальных). Теперь, если предположить, что существует возможность полиморфизма информации, то есть вероятность её маршрутизации, то начинается этап слияния свойств получения и отправления, образуя антиципацию. Так, например, если полиморфизм существует, значит будет существовать три этапа: (*A* → *B ИЛИ A* → *C*) → (*B* → *C ИЛИ C* → *B*) → (*B* → *A ИЛИ C* → *A*), но если полиморфизма не существует, то будет два этапа: (*A* → *B ИЛИ A* → *C*) → (*B* → *A ИЛИ C* → *A*)[5]. При этом предполагается, что системе известен лишь отправитель информации (инициатор), в то время как получатель не определён. Из этого следует, что если полиморфизм будет являться статичной величиной (то есть, будет всегда существовать или не существовать вовсе), то определение получателя будет являться лёгкой задачей (при условии, что он всегда отвечает инициатору). Но, если полиморфизм будет иметь вероятностную величину, то грань между отправлением и получением будет стираться, сливаться, инвертироваться, что приведёт к разному трактованию анализируемых действий: запрос(1) - ответ(1) - запрос(2) или запрос(1) - маршрутизация(1) -

[5] 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.

ответ(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. 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 *НОД(k, 2) = 2* (где *НОД* — наибольший общий делитель), то получим максимальную неопределённость, алеаторность при константе *k = 2*, которую можно свести к следующему минимальному набору действий полиморфизма: (*A → B ИЛИ A → C*) → (*B → C ИЛИ C → B*) → (*B → C ИЛИ C → B*) → (*B → A ИЛИ C → A*). В итоге все действия можно трактовать 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 приводит 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 этом случае, является лишь запрос(1), созданный инициатором связи, который будет трактоваться всегда детерминировано. Но и здесь стоит заметить, что при последующих действиях данная проблема всегда будет угасать из-за увеличивающейся энтропии, приводящей к хаотичности действий. Так например, на следующем шаге появится неопределённость вида запрос(3) = запрос(2) = маршрутизация(~2), означающая неоднозначность выявления отправителя. Итоговую модель можно представить следующим способом:

1.	(*A → B ИЛИ A → C*)	1, 2. [запрос(1)] →
2.	(*B → C ИЛИ C → B*) *ИЛИ* (*B → A ИЛИ C → A*)	1. [маршрутизация(1)] = 2. [ответ(1)] →
3.	(*B → C ИЛИ C → B*) *ИЛИ* ((*B → A ИЛИ B → C*) *ИЛИ* (*C → A ИЛИ C → B*))	1. [маршрутизация(~1)] = 2, 3. [запрос(2)] →
4.	(*B → A ИЛИ C → A*) *ИЛИ* ((*A → B ИЛИ C → B*) *ИЛИ* (*A → C ИЛИ B → C*)) *ИЛИ* ((*A → C ИЛИ C → A*) *ИЛИ* (*A → B ИЛИ B → A*))	1. [ответ(1)] = 2. [ответ(2)] = 3. [маршрутизация(2)] → …

Таким образом, задача шестой стадии анонимности формируется сложностью нахождения истинных субъектов информации при трёх и более пользователях не связанных между собой общими целями и интересами. 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 критерием уже образуется виртуальная маршрутизация, которая скрывает и разрывает связь объекта с его субъектами, приводит к зарождению шестой стадии анонимности.

При этом, стоит заметить, что в самой шестой стадии анонимности, на уровне ядра, заложен механизм постоянного умножения, приумножения энтропии, 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 невозможно выявление закономерностей под средством декомпозиции её составляющих.

4. «Подводные камни» шестой стадии анонимности

Анализируя сеть, базируемую на шестой стадии анонимности, 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 и 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, 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 (со стороны вероятности) обнаружению состояния пакета, а именно, является ли он запросом или ответом с вероятностью $^2/_3$, что эквивалентно более точному определению состояния субъекта информации.

Исходя из периода *T*, который вычисляется по формуле *НОК(2+k, 2)*, где *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 $^2/_3$ 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 транспорентным 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.

Т.к. сама проблема периода представляет собой лишь более вероятностный способ определения состояния, то для решения будет достаточным его повышение 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 $T = НОК(2, 1+2, 2+2, ..., n+2)$.

Теперь, если анализировать непосредственно сами пакеты, в моменты их перемещения по сети, то можно наблюдать точно заданную тенденцию при которой их размер стремится к уменьшению. Это связано с тем фактом, что сам пакет имеет свойство полиморфизма, которое инициализируется на отправляющей стороне и постепенно финализируется на пути к принимающей. Такая закономерность способна выявлять роль субъектов информации, при которой достаточно проанализировать лишь размер пакета с позиции двух отправлений $(A \to B) \to (B \to C)$ и если пакет, в таком случае, уменьшается на заведомо известную величину D[6], то это свидетельствует о крайне высокой вероятности, что сам узел B является только промежуточным получателем.

Чтобы решить данную проблему, необходимо рассматривать структуру пакета со стороны его размерности. Так например, если сообщение размером $S(P)$ создаётся на отправителе и сразу же шифруется всеми слоями размером равным $S(E)$, то результатом такой функции является размер полиморфного пакета $S(P) + S(E) = S(E(P))$. При этом, т.к. $S(E)$ предполагает собой все слои шифрования, то данный размер можно представить в виде суммы каждого отдельного шифрования, где $S(E) = S(E_1) + S(E_2) + ... + S(E_n) \to S(E_n(...(E_2(E_1(P)))...)) = S(E(P))$. При этом каждый отдельный слой шифрования $S(E_i)$ равен любому другому слою $S(E_j)$, что даёт тождество вида $S(E_1) + S(E_2) + ... + S(E_n) \equiv nS(E_1) = S(E)$. Таким образом, проблема представлена удалением каждого отдельного элемента $S(E_i)$ из общей суммы $S(E)$, что также приводит к постоянному уменьшению числа n на единицу и к детерминированному вычислению $D = S(E_i)$. Решением задачи является добавление пустой, неиспользуемой информации V_i случайного размера к каждому элементу $S(E_i)$, что, следовательно, приведёт к метаморфозу свойств детерминированности числа D, переходящего в алеаторность под средством неравенства $S(V_i \,||\, E_i) \neq S(V_j \,||\, E_j)$ и к невозможности представления размера $S(V \,||\, E)$ через выражение $nS(V_1 \,||\, E_1)$.

Хоть на данном этапе и невозможно определить число D, т.к. оно становится случайным, исходя из выражения $S(V_i \,||\, E_i)$, тем не менее, стремление полиморфного пакета к своему собственному разложению остаётся, а это говорит, что и остаётся возможным вероятностный анализ его размерности. Также, если идти от обратного и предположить, что существует отправление вида $(A \to B) \to (B \to C)$ и при этом, первый пакет оказывается меньше последующего, то данный факт говорит только о том, что второй пакет является самостоятельно сгенерированным и считается либо запросом, либо ответом, а узел B либо отправителем, либо получателем.

Одним из решений данной проблемы может являться создание отдельного поля в пакете, указывающего на следующего получателя (будь то истинного или промежуточного) с той лишь

---

[6] Детерминированная разница размеров пакета между шифрованной и открытой версией, имеющая единственный слой шифрования. Шифрованный пакет состоит из шифрованного заголовка, шифрованных данных (основной информации), шифрованной случайной строки, шифрованного сеансового ключа, шифрованного публичного ключа, хеша, шифрованной подписи и доказательства работы. При этом, динамическим размером обладает только поле с основной информацией, в то время как все остальные поля имеют статические размеры, что и приводит к возможности анализа пакета по динамике постоянного стремления к уменьшению, исходя из его константной дифференции.

$D = S(E(P)) - S(P)$,

где S - функция вычисления размера информации,
E - функция шифрования информации,
P - первоначальная информация.

целью, чтобы маршрутизатор мог дополнять пакет на некую величину размера M[7], приводящую к константному размеру K[8]. Данный способ удаляет вышеописанные проблемы полностью, но выдаёт промежуточным узлам дополнительную информацию о последующих получателях пакета, одним из которых станет истинный получатель. Критичный характер данной проблемы приведёт к негэнтропии, автоматической деградации шестой стадии, где будет существовать возможность формирования списка потенциальных получателей на основе ограничения диапазона множества узлов всей сети и приводящий к зарождению выходных нод, определённо знающих (или вероятностно распознающих) истинных получателей.

Другим решением данной проблемы является постоянное перенаправление пакета на псевдо-адрес отправителя, который вследствие всех процессов будет постоянно уменьшать размер пакета, добавляя при этом величину M, тем самым, приводя пакет к константной величине K. Так как адрес отправителя является симулятивным, то он никак не выдаёт адрес настоящий. Теперь предположим, что существует три узла $\{A, B, C\}$, где A является отправителем, а B или C - получателем, то вся концепция полиморфных действий приводится в следующем акте: $(A \rightarrow B$ *ИЛИ* $A \rightarrow C) \rightarrow (B \rightarrow A$ *ИЛИ* $C \rightarrow A) \rightarrow (A \rightarrow B$ *ИЛИ* $A \rightarrow C) \rightarrow (B \rightarrow A$ *ИЛИ* $C \rightarrow A)$ вместо $(A \rightarrow B$ *ИЛИ* $A \rightarrow C) \rightarrow (B \rightarrow C$ *ИЛИ* $C \rightarrow B) \rightarrow (B \rightarrow C$ *ИЛИ* $C \rightarrow B) \rightarrow (B \rightarrow A$ *ИЛИ* $C \rightarrow A)$. Проблемой такого подхода является отсутствие увеличения энтропии, т.к. само полиморфное состояние равновероятно и эквивалентно разбивается на два неполиморфных положения, которые в свою очередь полностью и однозначно выявляют истинного отправителя информации вне зависимости от количества этапов полиморфизма и вне зависимости от псевдо-адреса отправителя.

Ещё одним и более правильным способом решения проблемы является использование случайной величины R[9], вместо константной величины K. В то время как сама уязвимость и проблема образуется и воссоздаётся из детерминированности, то и константная величина K порождённая ей же, не способна в корне предотвращать схожие проблемы. На место величины K встаёт величина R, приводящая к хаотичности размерности пакетов, к диффузии детерминированных качеств и к неопределённому выявлению субъектов информации. Такой подход базируется на необходимости генерации вероятностного псевдо-пакета случайного

---

[7] Переменная величина M применяется для замещения удалённых слоёв шифрования, сохраняя размер любой стадии полиморфного пакета на уровне константной величины K.

$$M_n = \sum_{i=1}^{n} S(V_i \parallel E_i),$$

где $S(V_i)$ - размер случайной информации для каждого слоя шифрования,
$S(E_i)$ - размер отдельного слоя шифрования,
n - количество удалённых слоёв шифрования.

[8] Константная величина K является доминирующей концепцией большинства скрытых сетей, т.к. скрывает объём передаваемой информации под средством фиксации размерности пакета (объём может частично разглашать функцию пакета или его динамику, что является уязвимостью и приводит к необходимости её решения).

$$K_j = S(P) + \sum_{i=j}^{n} S(V_i \parallel E_i) + M_{j-1},$$

где j - стадия полиморфного пакета,
n - количество слоёв шифрования.

[9] Случайная величина R является противоположной концепцией константной величины K и представляет неопределённость отправления пакета со стороны маршрутизирующей стороны, где с вероятностью $1/2$ может быть создан и отправлен новый, «пустой» псевдо-пакет случайного размера, скрывающий, под средством алеаторности, дальнейший анализ динамики истинного пакета.

размера на маршрутизирующей или принимающей стороне. Таким образом, промежуточный/принимающий узел начинает становиться одновременно и псевдо-получателем для всех остальных участников сети.

Из вышеописанного также следует вывод, что если $X \in \{$*пакет меньшего размера, пакет большего размера*$\}$, а $Y \in \{$*отправитель/получатель, маршрутизатор*$\}$, то при их импликации $X_i \rightarrow Y_j$ все суждения будут являться ложными. Доказать хаотичность действий вероятностной величины R и неразрешимость детерминированного анализа можно следующими логическими выражениями:

1. Если новый пакет меньше предыдущего, то субъектом данного объекта является истинный отправитель, либо получатель.
Ложно, т.к. маршрутизатор может сгенерировать псевдо-пакет меньшего размера.

2. Если новый пакет меньше предыдущего, то субъектом данного объекта является маршрутизатор.
Ложно, т.к. ответ может быть меньше запроса. Если истинный ответ по логике приложения всегда больше запроса, то положение вероятностным образом меняется на обратное при использовании переменных величин $\{V_1, V_2, ..., V_n\}$.

3. Если новый пакет больше предыдущего, то субъектом данного объекта является истинный отправитель, либо получатель.
Ложно, т.к. маршрутизатор может сгенерировать псевдо-пакет большего размера.

4. Если новый пакет больше предыдущего, то субъектом данного объекта является маршрутизатор.
Ложно, т.к. ответ может быть больше запроса. Если истинный ответ по логике приложения всегда меньше запроса, то положение вероятностным образом меняется на обратное при использовании переменных величин $\{V_1, V_2, ..., V_n\}$.

Единственным побочным эффектом такого решения, является возможность одновременного появления сразу двух пакетов от одного узла в сети, что будет говорить только о факте маршрутизации или получения. Но данная проблема перестаёт таковой являться, если пакет меньшего размера будет отправляться спустя случайное количество времени после псевдо-пакета.

5. Анализ сетевых связей при шестой стадии анонимности

При анализе шестой стадии анонимности, при выявлении её «подводных камней» и способов их решения, во всех случаях в качестве базиса использовалась связь *все-ко-всем*, предполагающая, что исследуемые субъекты данной сети будут заведомо соединены друг с другом. Это в свою очередь приводит к игнорированию и абстрагированию иных возможных связей, способных существовать в реальности. Чтобы доказать безопасность оставшихся соединений, необходимо свести их ко связи *все-ко-всем*, тем самым, инкапсулировать множество свойств и неопределённостей в одно сингулярное, подвергаемое анализу состояние.

В общем случае существует всего три основных вида связей, в то время как все остальные соединения являются лишь побочными гибридами нижеприведённых видов.

1. *все-ко-всем* ($A \leftrightarrow B, A \leftrightarrow C, B \leftrightarrow C$) [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 шестой стадии анонимности, 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.

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 ↔ централизованная) ↔ (централизованная ↔ распределённая) ↔ (распределённая ↔ децентрализованная). При цикличности трёх элементов, инициализирутся 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 шестой стадии анонимности 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 репликация сообщения, а только после широковещательная связь.

Если предположить, что субъект *D* не способен генерировать информацию, а создан только 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 доказано ранее, шестая стадия невосприимчива к такому виду деанонимизации. Следовательно, узел *D* становится словно фантомом, несущественным прозрачным субъектом, не влияющим на безопасность и анонимность сети, базируемой на связи все-к-одному. Из этого также следует, что шестая стадия анонимности 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 имплозируя 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* для каждого отдельного субъекта, коим и является узел *D*, а это, в свою очередь приводит

к классическому (ранее заданному) определению шестой стадии анонимности. 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 под средством 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 расщепляется на две подсети {*A, B, C*} и {*B, C, D*}, мостом которой 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*.

6. Проблематика анонимных сетей

При существовании и полной реализации, а также доступности скрытых сетей, будь то основанных на пятой или шестой стадиях анонимности, проблема, связанная с мощностью доверия, возвращается. Это кажется парадоксальным, ведь сама задача ещё решилась на четвёртой стадии анонимности, когда мощность доверия становилась минимально возможной величиной. Сложность заключается именно в том, что при достижении пятой стадии анонимности, стремление к уменьшению мощности доверия начинает игнорироваться, становиться второстепенным и добавочным критерием, в то время как стремление к увеличению мощности анонимности начинает переходить в доминируемое состояние. Таким образом, осуществляется трансфузия двух свойств, где анонимные сети начинают инициироваться противоположным, инверсивным действием к четвёртой стадии анонимности, а именно — игнорированием анонимности (экзотеричностью) со стороны передаваемого объекта и её сохранением (эзотеричностью) в субъекте.

Не стоит также считать, что шестая стадия анонимности, объединяя два разных способа маршрутизации из двух стадий, сама по себе решает данную проблему. Скорее наоборот, шестая стадия напрямую наследует задачу от пятого этапа.

Сутью проблемы является именно возможность создания сервисов не основанных на четвёртой стадии анонимности, что приводит к возникновению приложений, представляющих угрозу информационной безопасности. Это связано с тем фактом, что анонимные сети представляют собой некую платформу сервисов и позволяют размещать приложения базируемые на клиент-серверной, многоранговой архитектуре, тем самым откатывая, регрессируя структуру защиты информации до второй стадии анонимности, делая её защиту централизованной, примитивной, а саму информацию транспарентной к серверному приложению.

В качестве примера можно привести сеть Tor. Доступ к сервису осуществляется вполне анонимно, но при этом сам способ хранения информации на данном приложении полностью зависит от его владельца. Это приводит к тому, что мощность доверия будет приближаться к обычному среднестатистическому сервису построенному на мощности анонимности равной единице. Иначе говоря, нет разницы, где приложение будет воссоздано, т.к. первоначальная проблема доверия будет оставаться в неизменно исходной форме.

Решить данный вопрос можно лишь ограничением допустимых сервисов со стороны самой скрытой сети. Таким образом, анонимная сеть в своей базе и основе должна быть имманентной и

имплозивной, содержать *N*-ое количество приложений построенных только на четвёртой стадии анонимности. Доступ к любым другим сервисам, не имеющих четвёртую стадию анонимности, или скрытым сетям, не реализующих безопасную архитектуру, должен быть закрыт и ликвидирован. Только методом агглютинации и интерференции, будет возможна синергия свойств анонимности и безопасности.

7. Тайные каналы связи

Секретные, тайные, эзотерические каналы связи - есть соединения, располагаемые в заведомо замкнутом, незащищённом, враждебном окружении и имеющие характеристики безопасной передачи информации. При этом анонимность, родственная скрытым сетям, не является базисом секретных каналов связи и, следовательно, может быть отброшена из-за ненадобности или по необходимости. Так, например:

1. Первым, минимальным видом анонимности в тайных каналах связи принято считать четвёртую стадию, то-есть сохранение экзотеричности субъекта и эзотеричности объекта, благодаря использованию криптографических методов преобразования информации. Но стоит также заметить, что такой принцип сохраняется и при использовании стеганографических методов [7], поскольку субъект остаётся открытым, а объект остаётся закрытым (только вместо сокрытия информации, скрывается сам факт её существования). Поэтому данный способ вполне корректно относить точно равным образом и к четвёртой стадии анонимности. При этом, если в секретных каналах связи используются именно криптографические методы, то они не ограничиваются только идентификацией субъектов (целостностью, аутентификацией), но также и применяют практику шифрования объектов (конфиденциальность). И так как тайные каналы связи разворачиваются в заведомо замкнутой системе (многоранговой), то и мощность анонимности в таком случае равняется единице.

2. Вторым, максимальным видом анонимности в тайных каналах связи принято считать шестую стадию, при этом пропуская, игнорируя, импутируя пятую. Вся особенность такого подхода заключается в невозможности использовать фактическую, реальную маршрутизацию, которую предполагает пятая стадия анонимности. Тем самым реальная маршрутизация отдаёт откуп виртуальной, существование которой возможно лишь и только на шестой стадии анонимности. Виртуальная маршрутизация имманентна, сводится к передаче объекта внутри единого, сингулярного приложения, связывающего всех субъектов изнутри. Таким приложением является сервер (или группа серверов с $|A| = 1$), при помощи которого клиенты передают друг другу и принимают друг от друга информацию. Так как приложение располагает полным знанием того, кто является отправителем и кто является получателем, то сам сервер становится создателем сети на основе которой располагается тайный канал связи. При всём этом, такое приложение, в задаче о тайных каналах связи, аналогично и равносильно государству, в задаче о построении анонимных сетей. Всё это ведёт лишь к единственно возможной борьбе за анонимность с приложением-создателем — методом спама (т.к. способ с федеративностью бессилен и недейственен в виртуальном пространстве).

Тайные каналы связи, использующие стеганографию, всегда имеют некий контейнер, в который помещается истинное сообщение. Под контейнером может пониматься ложное, неявное, сбивающее с пути сообщение, которое чаще всего носит нейтральный характер. Из этого также

следует, что в зависимости от размера контейнера, зависит и размер самого исходного сообщения, тем самым, стеганографический подход рассчитан на сообщения малых размеров и мало пригоден для передачи целых файлов. Примером контейнера может служить изображение, аудио-запись, видео-файл, то есть всё, что может хранить дополнительную или избыточную информацию, которая останется незаметной для человеческих глаз и ушей. Одним из примеров сокрытия информации может служить замена каждого старшего бита в изображении, битом исходного сообщения. Таким образом, если размер изображения (то есть, контейнера) будет равен 2MiB, то максимальный размер исходного сообщения не будет превышать 256KiB.

Тайные каналы связи, использующие криптографию, по умолчанию можно охарактеризовать четвёртой стадией анонимности. Если тайный канал разворачивается в заведомо замкнутой и незащищённой, но всё же сети, то это говорит о том, что стадия анонимности не меньше второй. Сами же секретные каналы данного вида используют идентификацию по криптографическим адресам, а не адресам, заданными системой по умолчанию (никнеймом, телефоном и т.д.), следовательно, стадия анонимности таких каналов определяется четвёртым этапом. Далее, если возникает виртуальная маршрутизация между субъектами, то четвёртая стадия начинает переходить в шестую, перешагивая при этом пятую. Таким образом, секретные каналы способны улучшать безопасность уже выстроенной и существующей системы в неизменном для неё состоянии, используя лишь и только её базис в качестве фундамента.

Использование стеганографии, вместе с криптографией, может помочь в случаях, когда имеется вероятность или возможность нахождения скрытого сообщения в контейнере. Тем самым, даже если исходное сообщение было найдено, оно будет иметь шифрованный вид. Здесь стоит учитывать тот факт, что при шифровании размер информации увеличивается (добавляется хеш, подпись, текст дополняется до блока), а из этого уже следует, что максимальный размер исходного сообщения уменьшается.

Существует ещё один, третий способ сокрытия информации, относящийся к криптографическим, но при этом обладающий некоторыми стеганографическими свойствами, качествами, особенностями [8, с.720]. Это не является последовательным объединением, использованием методов, как это было описано выше, а скорее оказывается их слиянием, синтезом, симбиозом. В таком методе истинная информация скрывается в цифровой подписи ложного сообщения на основе общего, согласованного ключа, где главной чертой и исключительностью является стойкость ко взлому, сродни сложности взлома цифровой подписи. При этом, сама подпись - есть контейнер, скрывающий существование сообщения методом аутентификации ложной информации.

Теоретически, тайные каналы связи также могут находиться и в других секретных каналах, либо анонимных сетях (т.к. тайные каналы могут быть воссозданы совершенно в разных системах и ситуациях), тем не менее, подобный подход является очень сомнительным (по причине избыточности накопленных слоёв шифрования), специфичным (по причине редкости практического использования) и затрачиваемым (по причине уменьшения производительности программ, уменьшения ёмкости контейнеров).

8. Протокол безопасной передачи информации

Из всего вышесказанного можно создать легковесный, примитивный, но при этом и безопасный протокол передачи информации, являющийся самодостаточным, цельным и монолитным. Может быть применим к анонимным сетям и тайным каналам связи [2, с.58][8, с.80].

Участники протокола:

A - отправитель,

B - получатель.

Шаги участника A:

1. $K = G(N)$, $R = G(M)$,

   где G - функция-генератор случайных байт,
   N, M - количество байт для генерации,
   K - сеансовый ключ шифрования,
   R - случайный набор байт.

2. $H_P = H(R \,||\, P \,||\, PubK_A \,||\, PubK_B)$,

   где H_P - хеш сообщения,
   H - функция хеширования,
   P - исходное сообщение,
   $PubK_X$ - публичный ключ.

3. $C_P = [E(PubK_B, K), E(K, PubK_A), E(K, P), E(K, R), H_P, E(K, S(PrivK_A, H_P)), W(C, H_P)]$,

   где C_P - зашифрованное сообщение,
   E - функция шифрования,
   S - функция подписания,
   W - функция подтверждения работы,
   C - сложность работы,
   $PrivK_A$ - приватный ключ отправителя.

Шаги участника B:

4. $W(C, H_P) = P_W(C, W(C, H_P))$,

   где P_W - функция проверки работы.
   Если $\neq$, то протокол прерывается.

5. $K = D(PrivK_B, E(PubK_B, K))$,

   где D - функция расшифрования,
   $PrivK_X$ - приватный ключ.
   Если расшифрование неверно, то протокол прерывается.

6. $PubK_A = D(K, E(K, PubK_A))$.

7. $H_P = V(PubK_A, D(K, S(PrivK_A, H_P)))$,

   где V - функция проверки подписи.
   Если $\neq$, то протокол прерывается.

8. $H_P = H(D(K, E(K, R)) \,||\, D(K, E(K, P)) \,||\, PubK_A \,||\, PubK_B)$,

   Если $\neq$, то протокол прерывается.

Данный протокол игнорирует способ получения публичного ключа от точки назначения. Это необходимо по причине того, чтобы протокол был встраиваемым и мог внедряться во множество систем, включая одноранговые сети, не имеющие центров сертификации, и тайные каналы связи, имеющие уже установленную сеть по умолчанию.

Безопасность протокола определяется в большей мере безопасностью асимметричной функции шифрования, т.к. все действия сводятся к расшифрованию сеансового ключа приватным ключом. Если приватный ключ не может расшифровать сеансовый, то это говорит о том факте, что само сообщение было зашифровано другим публичным ключом и потому получатель также есть другой субъект. Функция хеширования необходима для проверки целостности отправленных данных. Функция проверки подписи необходима для аутентификации отправителя. Функция проверки доказательства работы необходима для предотвращения спама.

Протокол пригоден для многих задач, включая передачу сообщений, запросов, файлов, но не пригоден для передачи поточной информации, подобия аудио звонков и видео трансляций, из-за необходимости подписывать и подтверждать работу, на что уходит много времени. Иными словами, протокол работает с конечным количеством данных, размер которых заведомо известен и обработка которых (то есть, их использование) начинается с момента завершения полной проверки.

Пример программного кода для шифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Encrypt(sender *PrivateKey, receiver *PublicKey, data []byte) *Package {
	var (
		session  = GenerateBytes(N)
		rand     = GenerateBytes(M)
		pubsend= PublicKeyToBytes(&sender.PublicKey)
		hash     = HashSum(bytes.Join(
			[][]byte{
				rand,
				data,
				pubsend,
				PublicKeyToBytes(receiver),
			},
			[]byte{},
		))
		sign = Sign(sender, hash)
	)
	return &Package{
		Head: HeadPackage{
			Rand:    hex.EncodeToString(EncryptS(session, rand)),
			Sender:  hex.EncodeToString(EncryptS(session, pubsend)),
			Session:hex.EncodeToString(EncryptA(receiver, session)),
		},
		Body: BodyPackage{
			Data:    hex.EncodeToString(EncryptS(session, data)),
			Hash:    hex.EncodeToString(hash),
			Sign:    hex.EncodeToString(EncryptS(session, sign)),
			Npow:    ProofOfWork(hash, C),
		},
	}
}
```

Шифрование подписи сеансовым ключом является необходимым, т.к. взломщик протокола, для определения отправителя (а именно его публичного ключа) может составить список уже известных ему публичных ключей и проверять каждый на правильность подписи. Если проверка приводит к безошибочному результату, то это говорит об обнаружении отправителя.

Шифрование случайного числа (соли) также есть необходимость, потому как, если злоумышленник знает его и субъектов передаваемой информации, то он способен пройтись методом грубой силы по словарю часто встречаемых и распространённых текстов для выявления исходного сообщения.

Пример программного кода для расшифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Decrypt(receiver *PrivateKey, pack *Package) (*PublicKey, []byte) {
	// Check proof.
	hash, err := hex.DecodeString(pack.Body.Hash)
	if err != nil {
		return nil, nil
	}
	if !ProofIsValid(hash, C, pack.Body.Npow) {
		return nil, nil
	}
```

```
// Decrypt session key.
eskey, err := hex.DecodeString(pack.Head.Session)
if err != nil {
	return nil, nil
}
skey := DecryptA(receiver, eskey)
if skey == nil {
	return nil, nil
}
// Decrypt public key.
ebpubsend, err := hex.DecodeString(pack.Head.Sender)
if err != nil {
	return nil, nil
}
bpubsend := DecryptS(skey, ebpubsend)
if bpubsend == nil {
	return nil, nil
}
pubsend := BytesToPublicKey(bpubsend)
if pubsend == nil {
	return nil, nil
}
pubsize := PublicKeySize(pubsend)
if pubsize  != KEY_SIZE {
	return nil, nil
}
// Decrypt and check sign.
esign, err := hex.DecodeString(pack.Body.Sign)
if err != nil {
	return nil, nil
}
sign := DecryptS(skey, esign)
if sign == nil {
	return nil, nil
}
if !Verify(pubsend, hash, sign) {
	return nil, nil
}
// Decrypt rand.
erand, err := hex.DecodeString(pack.Head.Rand)
if err != nil {
	return nil, nil
}
rand := DecryptS(skey, erand)
if rand == nil {
	return nil, nil
}
// Decrypt data.
edata, err := hex.DecodeString(pack.Body.Data)
if err != nil {
	return nil, nil
}
data := DecryptS(skey, edata)
if data == nil {
	return nil, nil
}
// Check hash.
check := HashSum(bytes.Join(
	[][]byte{
		rand,
		data,
		PublicKeyToBytes(pubsend),
		PublicKeyToBytes(&receiver.PublicKey),
	},
```

```
                []byte{},
        ))
        if !bytes.Equal(hash, check) {
                return nil, nil
        }
        return pubsend, data
}
```

Для улучшения эффективности, допустим при передаче файла, программный код можно изменить так, чтобы снизить количество проверок работы в процессе передачи, но с первоначальным доказательством работы на основе случайной строки (полученной от точки назначения), а потом и с накопленным хешем из *n*-блоков файла, для *i*-ой проверки. Таким образом, минимальный контроль работы будет осуществляться лишь $\lceil M/nN \rceil + 1$ раз, где *M* - размер файла, *N* - размер одного блока. Если доказательство не поступило или оно является неверным, то нужно считать, что файл был передан с ошибкой и тем самым запросить повреждённый или непроверенный блок заново.

9. Заключение

В данной работе были проанализированы скрытые системы, представляющие безопасность и безымянность пользователей, а именно — анонимные сети и тайные каналы связи. Была приведена градация анонимности в компьютерных сетях, базируемая на её мощности. На основе же градации было выявлено само развитие анонимности и необходимые условия для её существования. Основным, и пожалуй главным, моментом данной статьи является определение теоретической, абсолютной анонимности, базируемой на шестой стадии. Было найдено противоречие, при котором стремление к уменьшению мощности доверия становилось второстепенным свойством, как только достигалась пятая стадия анонимности. Решением проблемы стало объединение четвёртой стадии анонимности со стадиями высшего порядка. Из определения абсолютного анонимата была также выявлена возможность создания тайных каналов связи на базе шестой стадии анонимности, за счёт осуществимости применения виртуальной (вероятностной) маршрутизации. В части о тайных каналах связи было расширено определение четвёртой стадии анонимности, за счёт внесения стеганографических методов как возможной альтернативы криптографическим. В конце статьи был представлен протокол безопасной передачи информации, вместе с примерами программного кода, на основе которого могут базироваться в последующем анонимные сети и тайные каналы связи.

Список литературы

1. Диффи. В., М. Хеллман. Новые направления в криптографии [Электронный ресурс]. — Режим доступа: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 19.12.2020).
2. Шнайер, Б., Фергюсон, Н. Т. Практическая криптография / Б. Шнайер, Н. Т. Фергюсон. - М.: Издательский дом «Вильямс, 2005. - 420 с.
3. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.
4. Накамото, С. Биткойн: система цифровой пиринговой наличности [Электронный ресурс]. — Режим доступа: https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf (дата обращения: 19.12.2020).
5. Рябко, Б. Я., Фионов, А. Н. Криптография в информационном мире / Б. Я. Рябко, А. Н. Фионов. - М.: Горячая линия - Телеком, 2019. - 300 с.

6. Донован, А.А., Керниган, Б.У. Язык программирования Go / А.А. Донован, Б.У. Керниган. — М.: ООО «И.Д. Вильямс», 2018. - 432 с.
7. Шелухин, О.И., Канаев, С.Д. Стеганография. Алгоритмы и программная реализация / О.И. Шелухин, С.Д. Канаев. — М.: Горячая линия - Телеком, 2018. - 592 с.
8. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер. — СпБ.: ООО «Альфа-книга», 2018. - 1040 с.