Теория строения скрытых систем

Коваленко Геннадий Александрович

1. Введение

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 и логично, и оправдано, 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. Данная атака действительно значима и значительна, а также ссылается на нерешённую проблему доверия*, но в таком концепте анализа минимально рассматривается (а скорее даже игнорируется) возможность атаки со стороны самих субъектов A и B, разрушительная мощь которой может превосходить прямолинейные MITM атаки. Целью нашей статьи служит выявление данного метода атаки, его анализ и последующее решение.

Основной сутью проблемы является возможность атаки со стороны принимающей стороны. Так предположим, что субъект A есть отправитель, значит он автоматически становится жертвой нападения, если B есть получатель, он автоматически становится атакующим. Современная задача заключается в том, что истинным получателем информации (объекта) становится вовсе не пользователь B, а предположим, что участник C, в то время как сама точка B становится промежуточным, интерстициальным узлом, владеющим всей информацией о пользователях A и C (увлечениями, интересами, хобби, развлечениями, сообщениями, адресами) в предельно открытом, транспарентном состоянии. Узлу B известна совершенно вся передаваемая через него, и в последующем хранимая на нём, информация. Примером такого явления могут служить 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 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, симулякром, ссылающимся на несуществующую 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, 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 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**, чтобы собственная её структура представляла защиту объектов и анонимат субъектов. К системам подобного рода относятся анонимные сети и тайные каналы связи.

*Проблема доверия — невозможность построения безопасной и монолитной системы, основанной полностью на криптографических алгоритмах, без использования промежуточных субъектов, удостоверяющих идентификацию всех абонентов, либо сторонних каналов связи с заранее установленным доверием. Задача возникает на фоне сложности передачи публичных ключей. В децентрализованных 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.

**Мощность доверия — количество узлов, участвующих в хранении или передаче информации, представленной в открытом виде для данных узлов. 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.

2. 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.

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» (хоть и противоречиво), 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 сразу с несколькими другими. Децентрализованные же сети можно именовать «слабо централизованными» (хоть также и противоречиво), 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, монадой не представляющей собой саму анонимность, которая характеризуется её пустотой $|A| = 0$*. Примером может являться отсутствие связи как таковой или существование только прямого соединения между двумя одноранговыми субъектами, что равносильно их стазису.

2. Вторая стадия изменяет способ взаимодействия между субъектами, добавляя новую сущность в виде сервера. Таким образом, архитектура становится многоранговой, клиенты начинают пользоваться платформами связи, а мощность анонимности повышается до константного значения. Этап обеспечивает только анонимность клиент-клиент, но игнорирует при этом анонимность клиент-сервер, что приводит к статичной мощности

анонимности $|A| = 1$. Иными словами, сервер обладает достаточной информацией о клиентах (адреса, личные данные, интересы, хобби, развлечения, сообщения), но при этом сами клиенты общаются под средством сервера и не знают друг друга, а потому и являются анонимами. Типичным примером могут служить современные форумы, социальные сети, мессенджеры, иначе говоря, большинство сайтов и приложений, построенных на основе клиент-серверной архитектуры. Описанную стадию можно вкратце именовать псевдо-анонимностью.

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 $|A| \approx C$, где C - количество прокси-серверов. Хоть мощность анонимности действительно и повышается, 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 заменяет сетевой адрес криптографическим. Под заменой подразумевается частичное, неполное, фрагментированное преобразование, где сам сетевой адрес полностью не скрывается и никак не удаляется, он продолжает существовать в самом базисе, механизме компьютерных сетей, включая частично и последнюю стадию анонимности. Именно на данном этапе мощность доверия становится минимально возможной величиной, а потому и все приложения построенные 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) [3] 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, разрозненный характер поведения узлов, но при этом маршрутизация может нести дополнительный, добавочный фактор передачи информации, с последующим её сохранением и удерживанием на большинстве узлов сети, то-есть представлять слепую, заливочную трассировку [4, с.398]. При этом, в список задач такой маршрутизации не вносится как таковая анонимизация субъектов, она скорее представляет собой акцидентальное, второстепенное свойство. Поэтому, четвёртую стадию можно характеризовать игнорированием анонимности (экзотеричностью) со стороны субъекта и её сохранением (эзотеричностью) в передаваемом объекте. Мощность анонимности данного этапа чаще всего динамична, то-есть $0 < |A| \leq N$, где N - количество узлов в сети. Это связано с тем фактом, что предполагаемый получатель может оказаться на совершенно случайном узле, как близком к отправителю, так и дальнем от него, если учитывать, что маршрутизация действительно заливочная. В ином случае, трассировка может иметь также статичное количество узлов, как это происходило на третьей стадии анонимности, а именно $|A| \approx C$, где C - количество узлов участвующих в маршрутизации. Это в свою очередь не является ухудшением или каким бы то ни было улучшением анонимности в сравнении со слепой маршрутизацией. Выбор между способами роутинга обуславливается спецификой самого приложения.

5. Пятая стадия изменяет способ маршрутизации, придаёт ему свойство полиморфизма, изменчивости закрытой информации по мере перехода от одного узла к другому, при этом отстраняя 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, образуя тем самым новую, вероятностную (а также виртуальную) маршрутизацию. Данный этап объединяет 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.

Развитие анонимности можно представить и как становление пустоты в абсолют, проходимое через процессы снятия, как последовательные этапы отрицания, как триада — «тезис-антитезис–синтез», повышающая качество самой анонимности. Началом полагается одноранговая система (1 стадия), прямолинейная, примитивная, без какой бы то ни было анонимности, как тезис, который претерпевает этап отрицания под средством концентрации, становясь тем самым многоранговой системой (2 стадия) — антитезисом. Далее, многоранговая система начинает подвергаться своему отрицанию, т.к. знаменует своим существованием полную централизацию, отсутствие какой бы то ни было реальной анонимности. После данного отрицания появляются гибридные системы, объединяющие и соединяющие основные свойства одноранговых и многоранговых систем (3, 4 стадии), иными словами образуют их синтез. За этим сразу же следует, что гибридные сети, как отдельно взятый тезис, применяют на себя отрицание, т.к. не располагают целью саму анонимность, она для них является добавочным, второстепенным и неполным свойством. Отрицание в этом случае порождает антитезис, приводящий к частичному отмиранию гибридных систем, делающий сеть более раздробленной, распределённой, децентрализованной, однородной (5 стадия), и в конце концов, формирующий зачатки настоящей анонимности. Лишь последний этап отрицания, а следовательно, и финальный синтез, приводит всю систему к первоначально одноранговому состоянию, к полному отмиранию гибридности и к теоретически максимальной анонимности (6 стадия) за счёт объединения основных свойств тезиса и антитезиса.

Стоит также заметить, что шифрование, определяемое анонимностью, появляется частично лишь в моменты четвёртой стадии, в то время как во второй и третьей стадиях само шифрование является добавочным, дополнительным и второстепенным 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 информации, что, следовательно, ведёт к переходу на пятый этап.

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**. 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

пакета по сети. Рекуперация будет происходить до тех пор, пока не будет расшифрован последний пакет, предполагающий существование истинного получателя. Стоит также заметить, что маршрутизаторы при расшифровании пакета могут узнавать криптографический адрес отправителя, именно поэтому стоит отправлять транспортировочные пакеты из-под криптографического адреса псевдо-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)****. 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) - 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), ответ(2) = ответ(1), а также запрос(2) = маршрутизация(~1). 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), означающая неоднозначность выявления отправителя.

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.

* 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).

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

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.

** 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.

*** 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.

3. «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, дифференцированными, 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 выявить некоторые закономерности, приводящие к возможности точного обнаружения состояния пакета, а именно, является ли он запросом или ответом (при этом не разглашая субъектов 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 также являться запросом (аналогичная ситуация с ответом). Хоть и уязвимостей при данной детерминированности выявлено не было, тем не менее, с консервативной точки зрения, лучшим решением будет повышение периода, если атаки на этой основе будут обнаружены. Повысить период можно несколькими 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 $n < N$ (количество узлов в сети). Тогда период *T = НОК(2, 1+2, 2+2, ..., n+2)*.

Теперь, если рассматривать 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 $(A \rightarrow B) \rightarrow (B \rightarrow C)$ и если пакет, в таком случае, уменьшается на заведомо известную величину D^*, 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 $S(E) = S(E_1) + S(E_2) + ... + S(E_n) \rightarrow S(E_n(...(E_2(E_1(P)))...)) = S(E(P))$. 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 $D = S(E_i) = S(E_j)$. 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 $(A \rightarrow B) \rightarrow (B \rightarrow C)$ 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 целью, чтобы маршрутизатор мог дополнять пакет на некую величину размера M^{**}, приводящую к константному размеру K^{***}. 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 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 адрес псевдо-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 псевдо-отправителя является симулятивным, он никак не выдаёт адрес настоящий и при этом, сам принцип вероятностного полиморфизма не нарушается, а лишь туннелируется. 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: $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A) \rightarrow (A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$ вместо $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow C \text{ ИЛИ } C \rightarrow B) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$.

В итоге, вероятностный полиморфизм определяется как $(A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A) \rightarrow (A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A) \text{ ИЛИ } (A \rightarrow B \text{ ИЛИ } A \rightarrow C) \rightarrow (B \rightarrow A \text{ ИЛИ } C \rightarrow A)$, где запрос(1) = запрос(1), маршрутизация(1) = ответ(1), маршрутизация(~1) = запрос(2),

ответ(1) = ответ(2), запрос(2) = запрос(3) и т.д. Затем, если допустить, что при передаче осуществляется полиморфизм пакета, то его метаморфозы сводятся к следующим действиям:

Участники протокола:

A - отправитель,

B - маршрутизатор,

C - получатель.

Шаги участника A:

1. $C_{T1} = E(PubK_C, P)$,

   где *E* - функция шифрования,

   $PubK_X$ - публичный ключ,

   P - исходное сообщение.

2. $C_{T2} = E(PubK_A, [V_1 \,||\, PubK_C \,||\, C_{T1}])$,

   где V_i - случайная дополняющая величина.

3. $C_{P1} = E(PubK_B, [V_2 \,||\, PubK_A \,||\, C_{T2}])$,

   где C_{Pi} - зашифрованное сообщение ($lim_{CPi \to K}$),

   K - константная величина.

Шаги участника B:

4. $D(PrivK_B, C_{P1}) = V_2 \,||\, PubK_A \,||\, C_{T2}$,

   где *D* - функция расшифрования,

   $PrivK_X$ - приватный ключ.

5. $C_{P2} = E(PubK_A, [V_{2x} \,||\, C_{T2}])$,

   где $S(V_{2x}) = S(V_2 \,||\, PubK_A)$,

   S - функция вычисления размера информации.

Шаги участника A:

6. $D(PrivK_A, C_{P2}) = V_{2x} \,||\, C_{T2}$.
7. $D(PrivK_A, C_{T2}) = V_1 \,||\, PubK_C \,||\, C_{T1}$.
8. $C_{P3} = E(PubK_C, [V_{1x} \,||\, C_{T1}])$,

   где $S(V_{1x}) = S(V_{2x} \,||\, V_1 \,||\, PubK_C \,||\, E)$.

Шаги участника C:

9. $D(PrivK_C, C_{P3}) = V_{1x} \,||\, C_{T1}$.
10. $D(PrivK_C, C_{T1}) = P$.

В результате размерность всех стадий полиморфного пакета $(A \to B, B \to A, A \to C)$ представляет собой равнозначную величину, благодаря переменным величинам $\{V_1, V_2, V_{1X}, V_{2X}\}$ (внутри которых, как вшитый механизм, содержится регулирующая переменная *M*), которые приводят к возникновению и удержанию константой величины *K* на протяжении всего протокола для значений $\{C_{P1}, C_{P2}, C_{P3}\}$.

* 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 постоянному стремлению 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.

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

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

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

*** 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, что является уязвимостью и приводит к необходимости её решения). Противоположной концепцией константной величины является хаотичность размерности пакета, при которой информация дополняется некой случайной неконтролируемой величиной *R* на всех этапах полиморфизма. Из-за сложной доказуемости последней, в качестве основы, была взята концепция на основе константной величины.

$K = S(P) + lim_{S(V \parallel E) \rightarrow Ke}$,

где $Ke = L - S(P)$,
L - максимальный размер полиморфного пакета ($lim_{K \rightarrow L}$).

4. 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 средне-статистическому 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 иметь 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 таким образом, будет возможно органичное существование, в своём единении и в своей синергии, свойств анонимности и безопасности.

5. 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 недействен 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).

6. 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
	}
	// 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.

7. 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 (нереальной) 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.

8. 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. 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).
4. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.
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.