Теория строения скрытых систем[1]

Коваленко Геннадий Александрович

Аннотация. Существующие определения анонимности и безопасности конечных пользователей в сетевых коммуникациях часто являются расплывчатыми, неясными и противоречащими друг другу. Такая реальность восприятия стала следствием недостающей теоретической основы, которая могла бы структуризировать, и в некой степени даже стандартизировать, основные подходы к построению или использованию скрытых систем. Практическая реализация, которая далеко вышла за пределы теоретического понимания, становится в конечном счёте деструктивной и стагнирующей формой выражения скрытых систем, отодвигающая на второй план развитие их содержания. Понимание термина «анонимность», посредством декомпозиции его составляющих, способно дать оценку дальнейшего вектора развития анонимных и безопасных систем.

Ключевые слова: скрытые системы; анонимные сети; тайные каналы связи; клиент-безопасные приложения; сетевые коммуникации; сетевые архитектуры; стадии анонимности; теоретически доказуемая анонимность; криптографические протоколы; мощность анонимности; мощность доверия; мощность спама; централизованные сети; децентрализованные сети; гибридные сети;

Содержание

[1]Скрытые системы — множество сетевых технологий направленных на обеспечение и поддерживание приемлемого уровня анонимности конечных субъектов (отправителя и получателя) в совокупности с безопасностью объектов (информацией). При этом анонимность и безопасность могут реализовываться в разной степени, что делает класс таких систем достаточно обширным. К системам подобного рода относятся анонимные сети и клиент-безопасные приложения.

1. Введение

Вся история тайнописи, защиты информации, стеганографии и криптографии сопроваждалась антагонизмом двух сторон – нападающими и защищающими информацию как объект, передаваемый по линии или линиям связи [1][2]. В определённые промежутки времени брали вверх нападающие, когда все системы (во всём мире) становились полностью взламываемыми. В другие временные интервалы одерживали победу защищающие, когда таковые находили новые, более качественные способы защиты информации. В любом случае, атакующие представляли собой инициализацию всех последующих процессов, находивших уязвимости, недостатки определённых схем и эксплуатирующих их для получения нужных сведений. Всегда и во всей описанной истории нападающие играли двоякую роль – разрушения и созидания, когда с одной стороны, на базе краткосрочных интересов, их действия приводили к некоему отчаянию защищающих, понимающих бессмысленность и бесперспективность накладываемой безопасности, с другой стороны, уже на базе долгосрочных интересов, их действия приводили к полностью противоположным результатам – укреплению защищающих механизмов, где по мере понимания векторов нападения защищающие создавали иные, более качественные системы, противопоставляющие себя старым методам атак. Таким образом, вся история защиты информации являлась единством и борьбой противоположностей, в своём открытом, транспарентном представлении.

Сегодня, в настоящее время, если брать во внимание криптографию, как основной и базовый ориентир методов и средств защиты информации, то можно с уверенностью сказать, что защищающие полностью и абсолютно опережают атакующих. Во второй половине XX века криптография вышла из составляющей искусства (своей классической формы) и переродилась в полноценную науку (современную криптографию) благодаря работам Клода Шеннона, стандартизации шифра DES, открытию асимметричной криптографии, хеш-функциям и цифровым подписям. Все данные явления положительно сказались на разработке и переустройстве схем безопасности, когда в таком же всплеске начали зарождаться криптографические протоколы, пригодные для обширного множества частных и общих задач. Сейчас существуют такие алгоритмы и протоколы как AES, Serpent, RSA, Diffie-Hellman, Elgamal, SHA256, Keccak и т.д., эффективных алгоритмов взлома которых в настоящее время не найдено, даже спустя десятилетия их открытого криптоанализа с присущими вознаграждениями.

Вся вышеописанная информация, на первый взгляд положительная со стороны защиты информации, является на деле фиктивной, потому как нападающие сменили свои векторы нападения, слившись с защищающими. Плавное течение конкуренции и объединения атакующих и защищающих остановилось как только появился синтез средств массовой информации и компьютерных технологий. Атакующим более нет надобности в прямых взломах (по крайней мере в гражданском секторе), как того требовалось ранее. Нападающие в такой парадигме буквально разделились на два лагеря, где первые продолжили противостоять всё более новым средствам защиты информации, выбрав путь криптоанализа и развития квантовых технологий [3], а вторые выбрали путь взлома за счёт слияния со средствами массовой информации и её защищающими, став тем самым совершенно иной формой, отличной от примитивно атакующих и защищающих. Данная формация теперь одновременно и защищает, и атакует одних и тех же лиц, не совершенствуя (как это было ранее) средства защиты при обнаружении уязвимостей, потому как таковой стороне выгоден сам фактор незащищённости.

Вышеописанными атакующими (или защищающими) становятся сервисы связи (социальные сети, форумы, мессенджеры и т.д.), поток информации которых превосходит все оставшиеся виды коммуникаций. Защита информации клиентов обуславливается необходимостью её сдерживания от других сервисов. Нападение на информацию обуславливается необходимостью её продажи другим сервисам, либо выдачи государственному аппарату. Таким образом, будучи выдвигаемым сервисом связи, таковой противоречиво начинает выполнять две совершенно разнородные функции. Основной проблемой такого события становятся устаревшие модели угроз со стороны защиты информации, которые до сих пор акцентируют массовое внимание на новые или старые криптоаналитические атаки и на разработку квантовых компьютеров, которые дают лишь малый эффект, либо дадут таковой только в будущем. Сейчас же, мы имеем дело с куда более специфичной формой нападения, которая продолжает выполнять свои неявные функции.

В современных реалиях, обществом, будучи расположенным в виртуальном коммуникационном пространстве, всё сильнее начинает ощущаться нехватка настоящего уровня безопасности конфиденциальной информации и непосредственного уровня анонимности. Каждая компания, корпорация, правительство пытаются узнать и узнавать о человеке как можно больше разнородной информации – пол, вес, возраст, материальное положение, страна, город, улица проживания, политические взгляды, выбираемая одежда, отношения, друзья, родственники, телефон, электронная почта, биометрические данные, паспортная информация, устройство выхода в сеть, интересы, хобби, образование и т.д. Такая перемешанная масса данных связанных между собой лишь и только одним её субъектом становится ценнейшей информацией, выражающей человеческий капитал, отличительной особенностью которого становится репродукция потребления. Логичным интересом для «сборщика» такого рода информации становится её последующая продажа третьим лицам для получения экономической выгоды и экономического влияния. При монополизации или сговорных картелях таковых «сборщиков» становится возможным уже дальнейшее политическое влияние, направленное в первую очередь на подавление конкуренции и расширение системы, а также на сдерживание установленных и устанавливаемых императивов.

Изложение данной работы направлено на анализ становления таковых систем и на отличительные их особенности со стороны безопасности объекта (информации) и субъекта (пользователя, клиента системы). Из первичного анализа становится возможным выявление вектора развития последующих, более качественных сетевых коммуникаций. Большинство нижеизложенного материала проходит сквозь призму диалектической триады «тезис –

антитезис – синтез». Таковой подход позволяет выявлять не только лишь основные векторы развития будущих систем, но и их последующие качества, характеристики, как сочетания *N*-ого количества бывших парадигм. Помимо прочего, такой подход позволяет более детально рассматривать и ныне существующие системы, выявлять их недостатки, противоречия, способные играть роль в последующих деконструкциях и фазах отрицания. Поэтому само введение становится началом, истоком зарождения проблемы.

1.1. Этапы становления сетевых коммуникаций

Децентрализация, как первичная форма Интернет-коммуникаций в целом, появляется на фоне академических исследований [4, с.70], повлекших за собой глобальное развитие информационных технологий. Первичная система представляла собой не только внешний прогресс, относительно себя, но и имманентную эволюцию, выявляя в своей реализации отрицательные стороны и внутренние противоречия. Фактором её развития и одновременно гибели стала проблема масштабируемости связей типа «клиент-клиент». Невозможность в построении широковещательных и широкомасштабных соединений повлекли за собой потребность в промежуточных узлах, основаниях концентрации линий связи типа «клиент-сервер», тем самым, зародив ядро централизации, как точку отчёта дальнейшей проблематики.

Централизация, как вторая форма развития Интернет-коммуникаций, появляется на фоне разложения и отмирания первичной, децентрализованной оболочки [5]. Представляя свои плюсы масштабируемости, централизация начала претерпевать внутренние этапы развития, как итерации наложения слоёв абстракций и отрицания децентрализации, противоречиво став для последней фазой её собственной эволюции. При каждой новой итерации своего прогресса, централизованная система всё больше масштабировалась, всё сильнее углублялась корнями, всё чаще репрезентировала себя, образовывая тем самым симулякры [6, с.151] второго порядка. Одновременно с этим, система нейтрализовывала внешние атаки, ранее губительные для её ядра, но ныне безвредные для её функционирования, подобно атакам в обслуживании [4, с.869] (DDoS) или эксплуатации уязвимостей с учётом изъятия внутренней информации. С течением времени, продолжая развиваться и масштабироваться, система постепенно начала порождать общество всё более абстрагируемое от понимания её первичного механизма, всё более догматичное и фрагментированное. Инициатор системы становился её созерцателем, система становилась воспроизводством созерцателей. В итоге структура запустила собственную инициализацию своих внутренних интересов, инвертированно направленных на пользователей, тем самым кардинально изменив способ взаимодействия с ними. При выстроенном императиве, система начала образовывать множество симулякров третьего порядка ориентируемых на незначимость или сокрытие истинного уровня безопасности, подменяя реальность иллюзорностью происходящего в своём внутреннем слое за полями «сконфигурированных» абстракций. Итогом таковых ложных представлений стал «театр безопасности» [7], направленный на поддержание имеющегося порядка вещей (системы), с целью сокрытия реального уровня соблюдаемой конфиденциальности.

Внешние угрозы информационной безопасности хоть и становятся полностью безвредными для централизованной системы в ходе её постепенной и планомерной эволюции, но такое утверждение ничего не говорит об отсутствии внутренних угроз. Само масштабирование начинает порождать внутренние угрозы, быть противоречием системы, её развитием и конечным отмиранием. Всё большее расширение, продолжительная концентрация связей, неостановимая монополия соединений вызывают аккумулятивную

реакцию внутренних интересов её же участников. Внутреннему сотруднику компании теперь становится выгодно продавать информацию об её пользователях при всё большем расширении системы; государству становится выгодно концентрировать линии связи в одном сингулярном пространстве, в следствие возможности контроля за обществом и его деятельностью; рекламодателю становится выгодно вкладывать свои средства в массовую систему с наиболее релевантным алгоритмом выдачи рекламы на базе конфиденциальной информации клиентов, тем самым повышая свою прибыль [8][9]. И данная проблема информационной безопасности со стороны централизованных систем не может быть решена ей же, потому как она в своём базисе и самом ядре рассчитана на собственную масштабируемость и репрезентацию. Именно поэтому, жизнь централизованной системы прямо пропорционально начинает зависеть от количества слоёв абстракций, от количества копий без собственных оригиналов.

Гибридность, как третья форма развития Интернет-коммуникаций, отрицает централизацию, и в то же время, синтезирует её с децентрализацией. Оставляя масштабируемость, но отрицая внутреннее развитие централизации, происходит синтез внешнего развития децентрализации, как способа транспарентного доказательства функционирования без слоёв абстракций и симулякров третьего порядка. Такая система более невосприимчива к внутренним и внешним атакам, более нет внутреннего сотрудника, разглашающего информацию; государству становится не под силу эффективно собирать информацию; рекламодателю становится невыгодно вкладывать свои финансы. Подобный прогресс также несёт за собой и относительный регресс, потому как сама жизнеспособность системы начинает зависеть от участников выдвигающих себя на роль её поддержания, подобно энтузиастам, волонтёрам или, в лучшем случае, нодам, способных получать прибыть от донатов или внутреннего механизма (криптовалюты). В любом случае в таких системах более нет постоянного финансирования, а централизованные системы (в частности и само государство) начинают быть враждебными к её существованию [10]. Порождённость централизацией и враждебность к ней являются ключевыми факторами противоречия и главным фактом разложения гибридности, посредством её будущего разделения, расщепления, совершенствования.

Децентрализация, как четвёртая форма развития Интернет-коммуникаций, становится масштабируемой и одновременно безопасной средой для пользователей. Более не существует проблем гибридности, потому как ликвидировать систему централизацией с этого момента становится невозможным из-за её полностью ризоморфного характера, как отрицания иерархического. Любой пользователь становится в конечном счёте олицетворением самой системы, её участником и формой поддержания. На данном этапе безопасность информации начинает эволюционировать и переходить на более качественную ступень безопасности её субъектов. Система децентрализованная лишается всех своих первичных недостатков начальной формы и становится, в конечном счёте, снятием итераций отрицания в лице ранее забытого типа связи «клиент-клиент».

1.2. Централизация как фактор продолжительной стагнации

В настоящее время лидирующей формой выражения сетевых коммуникаций является вторая ступень развития. Централизованная оболочка становится наиболее долгоживущей средой, потому как таковая вбирает в себя наибольшее количество противоречий, парадоксально успешно сочетающихся между собой. Запутанность подобных связей отодвигает время их конечного распутывания посредством создания альтернативных решений. И действительно, предыдущая система и последующие представляют в неком роде

примитивы, явно обладающие своими преимуществами и недостатками, но что важнее всего – отсутствием противоборствующих сторон внутри самой системы.

В отличие от других систем, в централизованных явно прослеживаются два вида дифференцированных интересов, где с одной стороны находятся обладатели сервисов связи, с другой – пользователи этой системы. Первым становится выгодна такая парадигма вещей, потому как они овладевают всей информацией проходимой через них и хранимой у них. Это выгодно не только со стороны экономического влияния (реклама, продажа конфиденциальной информации, явные и неявныей подкупы и т.д.), но и со стороны политического контроля (пропаганда государственной или маркетинговой позиции, блокирование оппозиционных или «неправильных» мнений, явные и неявные шантажи, лоббирование интересов и т.д.). Само влияние, как тень, накладывается на субъектов подобных сервисов, поэтапно переводя их в категорию типичных объектов исследования рынка. Вторым становится выгодна парадигма использования сервиса без какой-либо нагрузки на своей стороне, с условиями хорошего соединения, большого хранилища и качественного дизайна UX/UI (user experience / user interface). Внешнее представление таковых действий становится с одной стороны неким описанием симбиоза, когда сервисы создают всю инфраструктуру для клиентов с целью своего будущего экономического и/или политического влияния, в то время как пользователи начинают использовать данную систему для комфортной взаимосвязи с другими её участниками. С другой стороны эти же действия становятся последующей формой паразитизма сервисов над её участниками, потому как вектор развития сервисов при достижении N-ого количества клиентов, некой критической массы, перевоплощается, интвертируется и становится, в конечном итоге, платформой связи живущей не для клиентов, а за счёт них. Теряя из виду причино-следственную связь жизнеспособности данного механизма, пользователи перестают осознавать на сколько масштабной начинает быть итоговая система сбора личной и конфиденциальной инфомации. Иронично (и печально), но именно таковые клиенты становятся единственной моделью противопоставления сервисам связи, единственной силой способной изнутри разрушать системы, живущие за счёт них, а не для них. Если таковые субъекты смогут не только найти, но и успешно перевести все свои возможные интересы на иные системы, представляющие близкие к ним стремления – интересы большинства, то централизованные механизмы постепенно и поэтапно начнут замещаться гибридными, децентрализованными альтернативами, начнут отмирать и, в конечном счёте, станут формой остатка всего множества сетевых коммуникаций.

В настоящее время можно наблюдать явный факт зарождения альтернативных систем, где гибридные становятся всё масштабнее в применении (Bitcoin, Tor), а децентрализованные в некоторых аспектах становятся даже более эффективным аналогом централизованных форм, на примере протокола BitTorrent при передачи файлов [11]. Такие действия должны были бы приводить к скорейшему отмиранию централизации как таковой, но в реальности этого не случается. Связано всё это с тем, что централизация обладает свойством долгоживучести, являющимся ключевым и многофакторным сценарием, обуславливаемым нижеизложенными составляющими.

Во-первых, явные интересы одних (прибыль, контроль) и абстрактные интересы вторых (коммуникация, поиск информации) приводят последних лишь к пассивным возражениям, бунтам без какого-либо сокрушительного результата. С другой стороны, как раз такое противоречие является наиболее важным, потому как оно инициирует медленное, поэтапное, но всё же развитие альтернативных решений. Примером такого поведения стала огласность проекта PRISM [12], которая смогла инициировать массовые недовольства населения всего мира, но при этом никакого фатального результата такая ясность не

принесла. До сих пор монополии и корпорации продолжают сотрудничать в равной степени с государственными аппаратами.

Во-вторых, комфортность использования сервисов начинает накладываться на текущий уровень безопасности, в некой степени отодвигая его на второй план, потому как конечные клиенты с большей долей вероятности выберут производительную систему, чем безопасную и медленную [13, с. 239].

В-третьих, сервисы преобретают свойство кажимости, имитации хорошего уровня безопасности, при этом даже к нему не стремясь. Централизованные сервисы не могут улучшить безопасность и сделать её более лучше, потому что они уже достигают наивысшего уровня защищённости в своей формации, последующие улучшения пойдут в явное противоречие со вторым пунктом – комфортабильностью.

В-четвёртых, централизации нет надобности и необходимости улучшать реальный уровень безопасности, если система смогла выстроить за счёт экономического влияния – политическое, в следствие которого штрафы за утечку информации становятся меньше стоимости найма специалистов по информационной безопасности [14].

В-пятых, централизованные системы по природе своей движутся к концентрации соединений, своеобразной монополии, из-за чего множество сервисов явным и неявным образом начинают объединяться, расширяться, срастаться, что приводит также к более успешным подавлениям иных систем, будь то гибридных или децентрализованных, а также малых централизованных. В определённой степени антимонопольные компании, являясь порождением централизованных механизмов, редко по настоящему и на практике противостоят монополиям [15][16][17].

В-шестых, экономический базис существования централизованных систем не позволяет выйти из существующего императива вещей, потому как сама централизация является лишь следствием экономической необходимости в управлении ресурсами, в том числе и человеческими. Разрыв парадигмы приведёт неминуемо к банкротству и последующему поглощению другой (более успешной) централизованной системой.

В-седьмых, централизованная форма является более гибкой системой при создании новых коммуникационных технологий, потому как игнорирует безопасность клиентской составляющей и располагает всей нужной пользовательской информацией. Таковые свойства позволяют ей куда быстрее разрабатывать новые решения, опережая на несколько шагов альтернативные системы.

В-восьмых, децентрализованные системы обладают свойством «коррозии» централизованными формами [19] (более подробно в подразделе «Движение моделей как развитие сетевых архитектур» раздела «Сетевые архитектуры и движение моделей»). Такое свойство является следствием высокой стабильности централизованных систем, при которой децентрализация всегда будет стремиться к выстраиванию более быстрых, качественных соединений за счёт установления *N*-ого множества стабильных или стабилизирующих узлов, что неминуемо будет приводить к концентрированию последующих соединений и относительному регрессу ризоморфных составляющих.

Таким образом, развитие постцентрализованных сетевых коммуникаций становится делом далёкого будущего. Противоречий накапливается с каждым разом всё больше, что продолжает играть двоякую роль. С одной стороны противоречия приводят систему к собственному отмиранию за счёт выявления явных недостатков, которые приходится постепенно решать и исправлять. С другой стороны большое количество накопленных противоречий также становится и фактором сдерживания к отмиранию системы за счёт необходимости в более длительном анализе её составляющих. В любом случае, на гниющей, разлагающейся и репрезентируемой, самовосстанавливающейся почве уже виднеются малые

ростки будущих сетевых коммуникаций, способных обеспечивать настоящий, а не фиктивный, уровень безопасности конечных пользователей, защищающий их личную и конфиденциальную информацию. Всё дальнейшее изложение нашей статьи будет акцентировано на анализе подобных систем.

1.3. Техническое описание основной проблематики

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 последнем. 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 [18]. Приведённая атака ссылается на нерешённую проблему доверия[2], разрушительную и губительную по своей сути, но при этом затмевающую более скрытую и деструктивную, мощь которой в современном мире превосходит прямолинейные MITM атаки. Одной из задач нашей статьи является выявление данного метода нападения, его анализ и последующие решения.

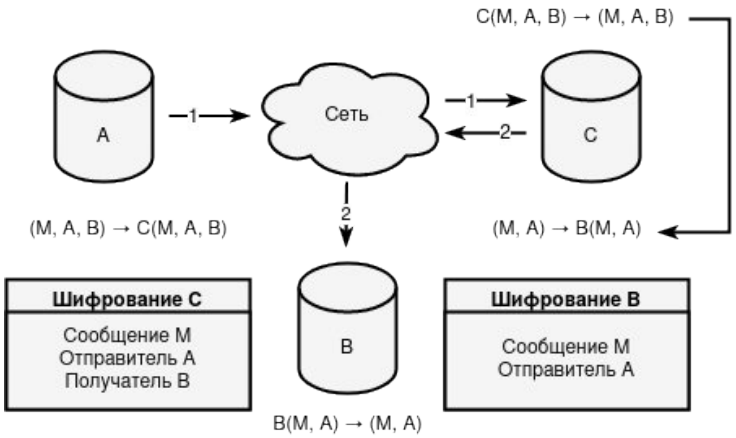

Рисунок 1. Коммуникация субъектов *A*, *B* посредством общего сервиса *C*

Возможность атаки со стороны принимающего субъекта есть суть проблемы, 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, как это изображено на *Рисунок 1*, целью которого является связывание двух и более клиентов между собой, образуя тем самым условно новый тип связи «клиент-клиент», который в свою очередь полностью игнорируется криптографическими протоколами. Такая проблема

[2]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.

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 [20][21]. 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 появлением раздела асимметричной криптографии [22]. 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, театром безопасности, симулякром ссылающимся на несуществующую, гипостазированную безопасность, как на магическое слово маркетинга, 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».

Таковое развитие приводит к возникновению систем доверия, где не только сами доверительные узлы становятся атакующими, но и промежуточные получатели, что приводит к куда более значительным и значимым рискам компрометации хранимых и передаваемых объектов между истинными субъектами. Эволюционируя, система начинает поддерживать неявные соединения между разнородными платформами связи, дублируя информацию на множество платформ с целью последующего массового сбора информации, обмена, маркетинга и продажи релевантной рекламы. В результате все вышеописанные факторы приводят к явному нарушению конфиденциальности конечных пользователей системы с определённым деанонимизирующим последствием.

Тем не менее безоговорочно аннигилировать такую систему доверия не представляется возможным из-за реального ухудшения оптимизации и производительности программ, последующих трудностей построения архитектуры приложений, и в конечном счёте, из-за невозможности полного искоренения доверия как такового [23, с.267]. Таким образом, необходимо не уничтожать, а заменять данную систему более безопасной, отодвигать её на второй план, в нишу, в которой только она способна быть полезной. Во всех других случаях, необходимо строить и разрабатывать иную систему, механизм которой стремился бы к уменьшению мощности доверия[3], в которой собственная её структура представляла бы

[3]Мощность доверия — количество узлов, участвующих в хранении или передаче информации, представленной дли них в открытом описании. 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 $|T| = 0$ будет возникать лишь

защиту объектов и анонимат субъектов. К системам подобного рода уже частично относятся анонимные сети, клиент-безопасные приложения и тайные каналы связи, анализ и развитие которых представлено в последующих разделах и подразделах.

2. Парадигмы сетевых коммуникаций

Все сетевые коммуникации строятся на определённых топологиях, архитектурах задающих последующее их применение. Топологию можно рассматривать как со стороны более низкого уровня, вида «звезда», «ячеистая», «шина», «кольцо» и т.п. [24], так и со стороны более прикладного уровня, как «многоранговая», «одноранговая», «гибридная» [25]. На первый взгляд, таковые определения дают однозначные соответствия: «многоранговая» = «звезда» ИЛИ «звезда + иерархическая» ИЛИ «иерархическая», «одноранговая» = «ячеистая» ИЛИ «полносвязная», «гибридная» = «иерархическая + полносвязная» ИЛИ «звезда + ячеистая» и т.д. Но по мере изучения будут явно прослеживаться противоречия таковых суждений, при которых «одноранговая» архитектура может становиться «звездой», «гибридная» – «иерархической» и прочее.

За основу терминологии сетевых архитектур будет браться именно прикладной уровень, т.к. низкоуровневый, в большей мере, описывает не как само взаимодействие субъектов между собой, а как способ технической коммуникации между таковыми точками. Если выбирался бы низкоуровневый подход в плане описания, то он несомненно порождал бы дополнительные противоречия, при которых, как пример, иерархическая система становилась бы системой децентрализованной. В это же самое время, многоранговая архитектура, изучающая взаимодействие субъектов между собой, предполагает, что таковая иерархичность как раз наоборот является следствием централизованности системы.

2.1. Определение сетевых архитектур

Многоранговые сети делятся на две модели: централизованные и распределённые. Централизованная или классическая клиент-серверная архитектура является наиболее распространённой моделью из-за своей простоты, где под множество клиентов выделяется один сервер, выход из строя которого приводит к ликвидации всей сети. Распределённая многоранговая система предполагает множество серверов, принадлежащих одному лицу или группе лиц с общими интересами, на множество клиентов, тем самым решая проблему уничтожения сети при выходе из строя одного или нескольких серверов. Из вышеописанного также следует, что классическая централизованная структура является лишь частным случаем более общей распределённой модели, или иными словами, сам факт распределённости становится следствием централизации. Сети на основе многоранговой архитектуры расширяются изнутри, относительно своего ядра, и не допускают расширения извне.

В одноранговых (peer-to-peer) системах все пользователи однородны, имеют одинаковые возможности, могут представлять одни и те же услуги маршрутизации [4, с.792]. Сами одноранговые сети могут быть разделены на три модели: централизованные, децентрализованные и распределённые (последние – условно). Централизованные

в моменты отсутствия каких-либо связей и соединений. Если $|T| = 1$, это говорит о том, что связь защищена, иными словами, никто кроме отправителя и получателя информацией не владеют. Во всех других случаях $|T| > 1$, что говорит о групповой связи (то-есть, о существовании нескольких получателей), либо о промежуточных узлах, способных читать информацию в открытом виде.

одноранговые сети представляют собой соединения на базе одного или нескольких, заранее выделенных или динамически выделяемых серверов-ретрансляторов, исключение которых приводит к блокированию всей сети. Отсутствие прав серверов в такой модели начинает порождать равноправность их клиентов. Распределённые сети не выделяют какой-либо центр или узел связи, сохраняя факт одновременной и полной коммуникации узла со всеми другими нодами, иными словами, со всей сетью (иногда под распределённой связью подразумевают необходимое *N*-ое количество соединений, необязательно со всей сетью). В децентрализованных же сетях возможно образование неравномерного распределения соединений и появление «неофициальных» узлов-серверов, часто используемых другими нодами в качестве последующей маршрутизации. Таким образом, децентрализованная модель в своём определении куда сильнее подвержена концентрированию линий связи, чем модель распределённая. Тем не менее, распределённая сеть является лишь конфигурацией децентрализованной и полноценно в отрыве от последней рассматриваться не может. Сети на основе одноранговой архитектуры расширяются извне, за исключением начальной фазы одноранговой централизации.

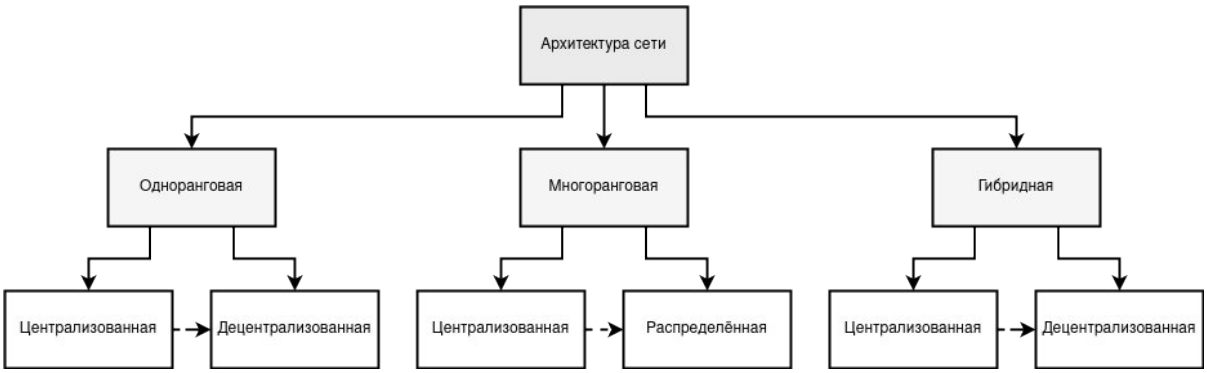

Рисунок 2. Сетевые архитектуры и их декомпозиция в моделях

Гибридная система объединяет свойства многоранговых и одноранговых архитектур, пытаясь взять и удержать как можно больше положительных и меньше отрицательных качеств (сама гибридность системы может рассматриваться в разных значениях и проявлениях, как пример на уровне топологий: «шина + кольцо», «кольцо + полносвязная», «звезда + ячеистая» и т.д., или на уровне прикладного рассмотрения: «одноранговая + многоранговая»). Плюсом многоранговых архитектур является возможность разделения логики на серверную и клиентскую, а также более быстрая и/или статичная скорость маршрутизации. Плюсом одноранговых архитектур может являться высокая отказоустойчивость за счёт внешнего расширения сети и возможность построения безопасной и масштабируемой «клиент-клиент» связи. Минусом гибридных архитектур на ранних стадиях развития является их возможный, осуществимый и более вероятностный переход в многоранговые системы (по сравнению с одноранговыми) за счёт большого уплотнения серверов принадлежащих одному лицу, либо группе лиц с общими интересами.

2.2. Движение моделей как принцип развития

Развитие сетевых архитектур в плане синтеза безопасности и анонимности проходит в следствие движения принадлежащих им моделей. Весь нижеизложенный анализ данного раздела будет действенен только в пределах исторически-длительного развития скрытых систем и не пригоден к обширному историческому анализу всего развития одноранговых,

многоранговых или гибридных сетевых архитектур в целом. Так например, если отбросить определения безопасности и анонимности, а взять в качестве основы только сетевые коммуникации, то ARPANET, являясь первой формой одноранговой децентрализации, порождает сеть Интернет, которая становится второй, финальной, эволюционированной формой одноранговой децентрализации, что на корню противоречит нижесказанному. Также, если исходить только из безопасности, игнорируя при этом полностью или частично анонимность, то исторически сеть Napster, являясь одноранговой централизованной моделью, моментально (после своего отмирания) порождает сеть Gnutella, как синтез многоранговой и одноранговой централизации, что также противоречит части нижесказанного, потому как исключает фазы и этапы возникновения гибридных архитектур. Далее, если же исходить только из анонимности, игнорируя безопасность, то исторически становится невозможным целостное определение многоранговой архитектуры, потому как таковая, становясь отрицанием анонимности, становится одновременно и её исключением. Через исключение в свою очередь становится невозможным целостное рассмотрение многоранговой распределённой модели, потому как таковая в своей совокупности начинает уже содержаться в гибридных архитектурах, которые и становятся способными самостоятельно воссоздавать первично качественную анонимность, что является непосредственным противоречием. Таким образом, весь нижеизложенный материал необходимо пропускать через призму развития безопасности и анонимности как единого неразрывного целого.

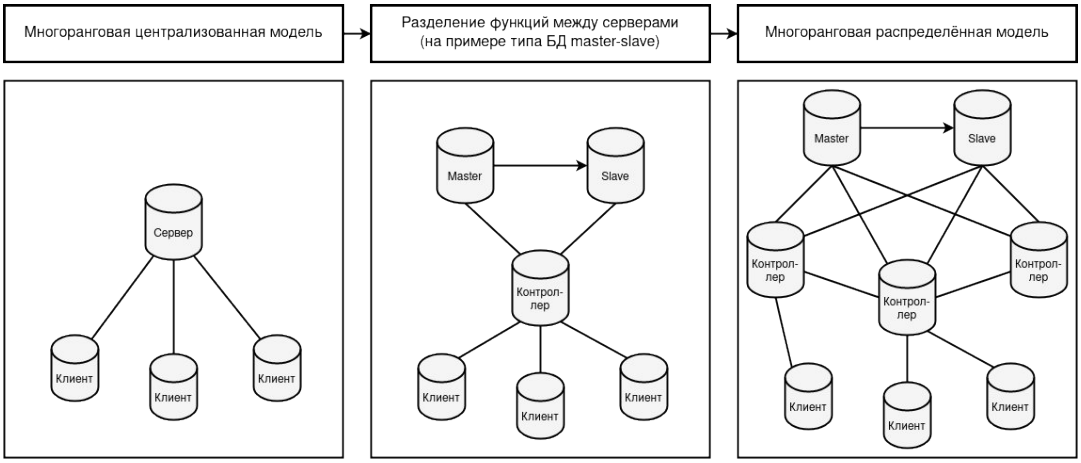

Рисунок 3. Развитие многоранговой архитектуры на примере типа БД «master-slave»

Становление многоранговой централизованной (классической) системы является следствием отрицания одноранговой начальной децентрализованной модели, как формы нежизнеспособной к нарастающим реалиям масштабируемости. На данном этапе одноранговый узел, словно единая личность, расщепляется (чтобы собраться вновь) на два субъекта – клиента и сервера. Таковое разделение предполагает разграничение прав между обработкой информации со стороны сервера и её инициализацией со стороны клиента. В подобной системе информация становится отчуждённой от её первичного создателя и переданной в «руки» сервиса хранения. Клиентам, в такой парадигме, становится избыточно, проблематично (и даже архаично) создавать прямолинейные связи между друг другом, потому как их информация благоприятно начинает переходить в удобочитаемое и отсортированное состояние без добавочных проблем и трудностей в плане ручной настройки соединений и способа хранения данных. Инициализация единой точки отказа становится главным фактором развития иерархичности, но никак не точкой сопутствующего

разрушения, как это было с первичной децентрализацией, когда таковая не могла эволюционировать без собственной деструктуризации. Когда многоранговая классическая, централизованная система начинает нести бремя значительных рисков компрометации всей хранимой информации она прогрессирует, вбирая в себя частично свойства первичной децентрализации и подстраивая их под собственный императив. Таким образом начинают зарождаться многоранговые распределённые системы.

Становление многоранговой распределённой системы из классической централизованной является важным составляющим фактором эволюции существующих иерархических сетей. Данное «разложение», как отрицание явной централизации, начинается на этапе разделения функций, приравнивая сервер к определённому действию, как это изображено на *Рисунок 3*. В такой начальной фазе, сервера становятся взаимосвязанными общей целью обслуживания, но не скованными выполнением общих задач. Из этого следует, что отказ в обслуживании одного сервера начинает влиять только на частную задачу (текущего сервера) и продолжает влиять на общую цель (группы серверов). Таким образом, затрагивая один сервер, сама система продолжает функционировать, хоть и не выполняя полный спектр запланированных действий. Последующей фазой развития уже становится взаимозаменяемость серверов, выполняющих узкоспециализированную задачу, посредством их дублирования, тем самым решая проблему отказоустойчивости в целом. В данном контексте стоит заметить, что иерархичность структуры продолжает сохраняться, даже при добавлении множества серверов с однородными функциями, не перерастая в одноранговую систему полноценно. Представленное явление проходит в следствие внутреннего алгоритма расширения системы, доступ к которому осуществляется наиболее высшими звеньями уже существующей и выстроенной иерархической цепи, а также в следствие бессмысленности существования узкоспециализированных одноранговых узлов вне всей системы. Поэтому, даже если внутри централизованных систем будет существовать *N*-ое количество одноранговых, сама сеть не перестанет быть многоранговой, до тех самых пор, пока будет существовать механизм восстановления и удержания иерархичности, а также до тех пор, пока одноранговые узлы будут оставаться специализированными конкретным задачам. Т.к. иерархичность в любом своём проявлении порождает централизацию, то во всех последующих упоминаниях под термином «централизация» будет пониматься именно конечная фаза эволюции многоранговой архитектуры — распределённая модель.

Становление одноранговой централизованной системы является следствием «переосмысления» многоранговой централизации, её отрицанием. Инвертируя способ взаимодействия между клиентом и сервером, данная модель делает последнего лишь держателем сети, придатком коммуникаций. В такой системе все пользователи становятся однородными и равноправными только за счёт отсутствия прав сервера, главной функцией которого, в конечном счёте, становится перенаправление пакетов между клиентами сети. Вследствие этого, сервера в одноранговой централизации лишаются дополнительных прав многоранговой архитектуры, лишаются быть полноценными посредниками между несколькими субъектами, тем самым и лишаясь функций сохранения, обработки и выдачи получаемой информации. При поверхностном анализе, централизация одноранговая, как этап развития сетевых коммуникаций, становится лишь упрощением централизации многоранговой. При более же углубленном анализе выявляется, что таковая модель способна не только дублировать сервера практически в неограниченном количестве (за счёт отсутствия какой бы то ни было логики кроме ретрансляции), что частично отсылает нас к способу функционирования многоранговой распределённости, но также и расширяться извне, что присуще одноранговым архитектурам. Таким образом, можно утверждать, что

одноранговая централизация становится альтернативным вектором развития многоранговой централизации.

Становление одноранговой (финальной) децентрализованной системы не является прямым следствием развития централизованной модели. Централизация одноранговая по историческим причинам способствовала инициализации децентрализованной философии, но не за счёт последовательных этапов улучшения, а за счёт фактора нежизнеспособности, слабости в «сожительстве» с многоранговой системой [26] в начальной фазе своего существования. Последняя в буквальном смысле «поглотила» примитивную одноранговую централизацию, привела к концентрированному методу выстраивания связей и иерархическому способу существования системы. Таким образом, децентрализованная модель должна была стать более качественным выражением и проявлением одноранговой архитектуры, чем централизованная. Итогом такого процесса стало объединение клиентской составляющей с серверной частью, породив тем самым узлы связи, как отдельные сетевые единицы коммуникации, возникшие из эволюции гибридных архитектур. Частным случаем продолжительного развития одноранговой децентрализации является становление распределённой системы, как следствия нарастающей концентрации линий связи со стороны децентрализованной модели, претерпевающей этапы «коррозии» централизацией и приводимой к возникновению «узких» мест среди нескольких сетевых множеств. Противоречием децентрализованных моделей является их постоянное движение к сосредоточению соединений, от хаотичности к порядку, от безопасности к отказоустойчивости, — таковыми становятся основные векторы регресса децентрализации основанные на выборе наиболее стабильных узлов. Решением становится иная и более качественная концентрация линий связи, основанная на объединении узлов посредством многочисленных соединений, в противовес единому центру коммуникаций, и как следствие, фактор стабильности возобновляется уже в количественном выражении узлов.

Становление гибридной архитектуры проходит в следствие синтеза одноранговой централизации и многоранговой распределённости. С одной стороны, одноранговая централизация частично избавляет систему от ядра внутренней иерархии, разбавляя её внешними одноранговыми связями. С другой стороны, многоранговая распределённость преобразовывает примитивные редирект-функции, изменяя их форму дополнительными действиями, и тем самым сохраняет внешнюю иерархию между сервером-клиентом. Внешним противоречием гибридности, на первый взгляд, становится сильная схожесть либо с многоранговыми распределёнными моделями, либо с одноранговыми децентрализованными. В совокупности же, гибридная архитектура представляет собой скорее переходное состояние, то-есть фазу развития систем и их моделей, нежели собственное и статичное положение. И действительно, гибридная архитектура описывается как синтез одноранговой централизации с многоранговой распределённостью, являясь причиной их последующей негации, приводимой уже к определению децентрализованной модели одноранговой архитектуры, как единовременного отрицания одноранговой централизации и многоранговой распределённости, то-есть отрицания гибридности. Именно поэтому, гибридная архитектура на этапе своего становления имеет больше свойств схожих с централизацией, где отличительной особенностью данной модели становится способность к единовременному внешнему (свойственно одноранговым архитектурам) и внутреннему (свойственно многоранговым архитектурам) масштабированию. В последующем, по мере своего развития, гибридность претерпевает ряд метаморфозов и становится в конечном счёте неотличимой (относительно некоторого множества субъектов) от децентрализованной модели. Это можно наблюдать на примере сетей Tor и Bitcoin, которые являясь одновременно гибридными, представляют разнородный вид гибридности, где в одном случае

Tor более приближен к распределённой модели многоранговой архитектуры (централизованной модели гибридности), а Bitcoin к децентрализованной модели одноранговой архитектуры (децентрализованной модели гибридности).

Метаморфозы сетевых моделей кратко представляются через призму детерминированного конечного автомата, изображённого на *Рисунке 5*, состояния которого изменяются по мере исторической на то необходимости и направленности. Так например, действия (*a*, *d*, *g*) можно рассматривать как необходимость в переосмыслении, во внешнем отрицании, (*b*, *f*) – необходимость в развитии, во внутреннем отрицании, (*c*+*e*) – необходимость в объединении, в синтезе отрицаний. Из всего вышеприведённого возможно составить выражения, относящиеся к развитию каждой определённой модели, где многоранговая централизация = (*a*), многоранговая распределённость = (*ab*), одноранговая централизация = (*ad*), гибридная централизация = (*abc*+*ade*), гибридная децентрализация = (*abc*+*ade*)(*f*) и, в конечном итоге, одноранговая децентрализация = (*abc*+*ade*)(*fg*).

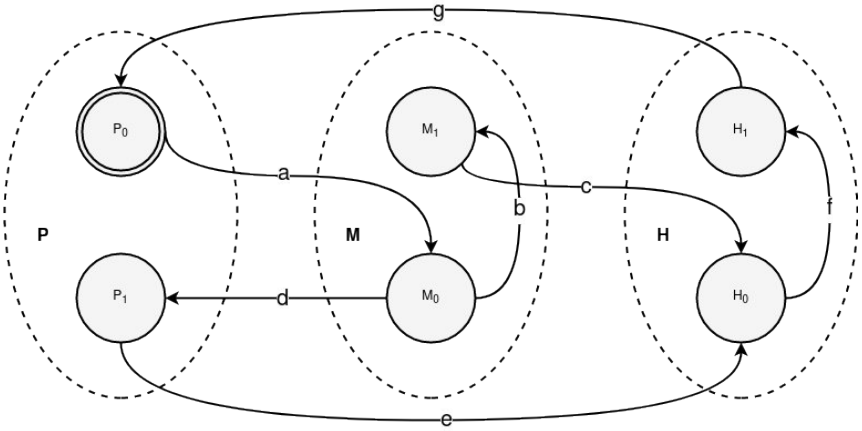

Рисунок 5. Конечный автомат развития сетевых архитектур посредством движения их моделей, где {P, M, H} – сетевые архитектуры: P – одноранговая, M – многоранговая, H – гибридная

Также стоит отметить, что развитие децентрализованной модели не является примитивно однородным, как это может показаться на первый взгляд, потому как таковая система в своём историческом понимании приобретает двойственное значение. С одной стороны, децентрализация становится первичной формой сетевых коммуникаций, инициализацией и точкой отчёта всех последующих архитектурных решений. С другой стороны, децентрализация, посредством этапов отрицаний и снятия, начинает быть более совершенной формой, и в конечном счёте выражением финализации форм движения сетевых архитектур. Таким образом, по исторически-закономерным причинам, первичная децентрализация вырождается только в многоранговую централизацию, а конечная её форма — в более высокую стадию децентрализации. В итоге децентрализация становится замыканием всего сетевого развития, одновременно являясь его началом и финалом.

3. Определение скрытых систем

Скрытые системы представляют собой общий и обширный класс сетевых коммуникаций способных поддерживать анонимность субъектов и безопасность передаваемых объектов. В определённой степени таковые системы могут быть нацелены на безопасность передаваемых объектов в степени большей, отодвигая анонимность на второй план, либо наоборот, делая систему анонимной, но полноценно не заботясь о безопасности

объекта после получения точкой назначения. Но так или иначе, в любом из представленных случаев таковые системы полноценно никогда не исключают свои второстепенные качества, что даёт возможность определённых комбинаций. При данных композициях сочетаются свойства и безопасности, и анонимности, что делает таковые системы полными. Полные скрытые системы, в свою очередь, являются решением основной проблематики данной работы.

3.1. Анонимные сети

Скрытые, тёмные, анонимные сети — есть сети, 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 [4, с.912]. Таким образом, только в совокупности этих двух свойств сеть может являться скрытой [27][28].

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 [29]. Именно по историческим причинам, современные скрытые сети имеют оверлейные уровни безопасности.

Любая анонимная сеть основывается либо на одноранговой (ризоморфной), либо на гибридной (комбинированной) архитектуре сети, исключая при этом многоранговую (иерархическую). Последняя архитектура является прямым отрицанием анонимности, направленным на её подавление посредством концентрации линий связи. Гибридная архитектура совмещает в себе некоторые свойства многоранговой и одноранговой архитектур.

По скорости и способу распространения информации выделяют два вида анонимных сетей – с низкими и высокими задержками [30]. Системы с низкими задержками ставят в качестве базовой необходимости скорость, эффективность транспортирования информации между истинными её субъектами, при этом уровень анонимности таковых сетей недостаточен для противопоставления атакам со стороны внешних глобальных наблюдателей (как фактора сильной анонимности). Системы с высокими задержками ставят в качестве базовой необходимости реальный уровень анонимности, в том числе и направленный на противодействие глобальным наблюдателям, но при этом скорость передачи становится в таковых сетях самым главным недостатком. Из вышеописанного следует классическая проблема проектирования безопасных систем – выбор компромисса между производительностью и безопасностью. В качестве примеров систем с низкими задержками выделяют Tor, I2P, Tarzan и т.д., а с высокими задержками – Mixminion, Herbivore, Dissent и т.п.

Маршрутизация в анонимных сетях не является примитивной и ставит эффективность распространения объектов на второй план, потому как главной целью становится создание запутывающего алгоритма (анонимизатора), который приводил бы к трудоёмкости анализа истинного пути от точки отправления до точки назначения. Производительность, эффективность «чистой» маршрутизации теряется, заменяясь особенностью алгоритма. В таких условиях, сами скрытые сети становятся медленными и сложными в применении (в

том числе и с низкими задержками), что также частично или полноценно отодвигает их прикладное и повседневное использование в настоящее время.

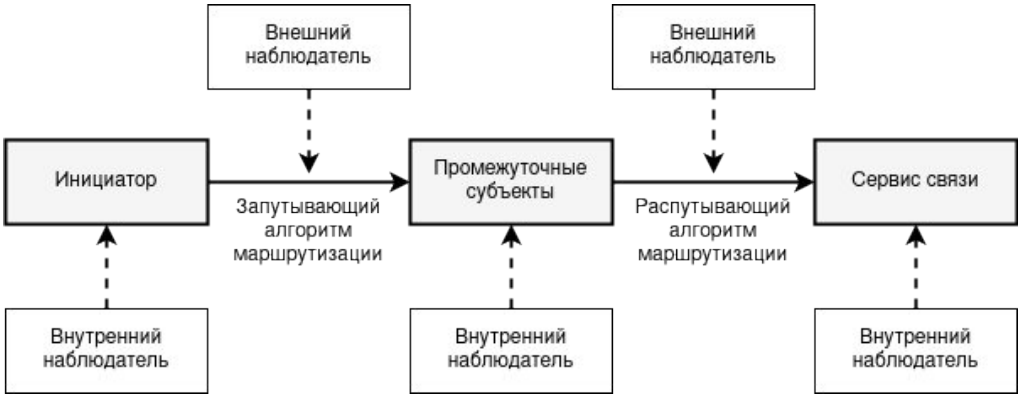

Рисунок 6. Внешние и внутренние наблюдатели (атакующие) в критериях запутывающего алгоритма маршрутизации

В задачах такого типа маршрутизации лежат модели угроз, в которых учитываются возможности атакующих. Главным антагонистом в подобных условиях становится государство, как внешний, глобальный наблюдатель, способный просматривать в широком масштабе распространение объектов по сети. В таком случае алгоритм маршрутизации должен уметь запутывать внешнего противника, не предоставлять возможности выявлять закономерности отправления, получения, запросов и ответов участниками анонимной сети. Другими, и не менее серьёзными противниками, являются внутренние атакующие, когда сами её же участники становятся отрицанием системы, её разложением. Предполагается, что внешние наблюдатели, помимо анализа трафика сети, способны также блокировать работающие узлы в системе, тем самым рассматривая их уникальные комбинации и паттерны поведения. Внутренние же наблюдатели способны наполнять сеть кооперируемыми узлами и совершать помимо маршрутизации также дополнительные действия, как отправление и получение информации. Наблюдатели без дополнительных функций называются пассивными атакующими, в противном случае – активными. В таких реалиях алгоритм маршрутизации должен отстранять буквально каждого субъекта (отправителя, получателя и промежуточного) от полноценного анализа принимаемых и отправляемых пакетов.

В своей совокупности, в синтезе, сговоре внешних и внутренних атакующих, способны проявляться атаки, которые ранее были бы невозможности по отдельности. Абстрагировано, основные методы нападений, как множества, можно изобразить в виде *Таблицы 1*. При этом, из определения активных атак выясняется, что таковые являются надмножеством пассивных, то-есть $A \in C$ и $B \in D$.

	Внутренние атаки	Внешние атаки
Пассивные атаки	A	B
Активные атаки	C	D

Таблица 1. Пассивные / Активные и Внутренние / Внешние нападения как множества векторов направленных на анонимные сети

Скрытыми сетями с теоретически доказуемой анонимностью принято считать замкнутые (полностью прослушиваемые) системы, в которых становится невозможным

осуществление пассивных атак с минимальными условностями по количеству узлов неподчинённых сговору. Говоря иначе, с точки зрения пассивного атакующего, апостериорные знания (полученные вследствие наблюдений) должны оставаться равными априорным (до наблюдений), тем самым сохраняя равновероятность деанонимизации по N-ому множеству субъектов сети.

Из специфичной формы маршрутизации выявляются критерии на основе которых можно утверждать, что сеть является анонимной. Так например, сети Tor, I2P, Mixminion, Herbivore и т.п. являются анонимными сетями, потому как обеспечивают анонимность субъектов, за счёт запутываемой маршрутизации, и безопасность объектов в коммуникациях между инициаторами и платформами связи. Сети RetroShare, Freenet, Turtle, Bitmessage и т.п. не являются анонимными сетями, т.к. маршрутизация представляет собой только сам факт передачи (в некой степени и специфичный из-за гибридного или однорангового характера сетевой архитектуры), транспортирования информации без непосредственного применения запутывающего алгоритма, хоть самолично системы и обеспечивают высокий уровень безопасности объектов. Не являются скрытыми сетями также и сети предоставляющие исключительно анонимность субъектов в отрыве от безопасности передаваемых объектов. Такое событие крайне специфично, но возможно на примере «чистых» DC-сетей, как неклассических форм первой стадии анонимности (более подробно в подразделах «Формы становления сетевой анонимности» и «Двойственность первой стадии анонимности»).

3.2. Клиент-безопасные приложения

Клиент-безопасные приложения или приложения базируемые на безопасной линии связи «клиент-клиент» представляют собой абстрагирование передаваемых / хранимых объектов от промежуточных субъектов, тем самым приводя мощность доверия $|T|$ к своему теоретически минимально заданному значению. В таких условиях, клиент-безопасные приложения являются ключевым фактором в построении тайных каналов связи. Частным случаем связи «клиент-клиент» становится сквозное (end-to-end или E2E) шифрование [20].

Основным следствием пониженной мощности доверия является возможность доказательства безопасности приложения ориентируясь только на его клиентскую составляющую. Это в свою очередь говорит, что ранее существующие сервера, как сервисы связи, теперь являются лишь промежуточными узлами, созданными для транспортирования, маршрутизации, либо хранения информации в полностью зашифрованном или аутентифицированном виде. Любое редактирование существующей или создание ложной информации на стороне сервиса будет сразу же обнаружено клиентской составляющей.

Одной из основных особенностей таких систем является криптографическая идентификация субъектов информации. Так как подобные системы более не являются многоранговыми, то субъекты становятся неспособными применять в чистом и привычном виде схемы типа «логин/пароль» в целях своей авторизации. Авторизация и последующие аутентификации относительно всех клиентов сети выявляются из асимметричной пары ключей. Публичный ключ (или его хеш) становится в конечном счёте идентификацией субъекта, а все посылаемые пользователем сообщения подписываются приватным ключом, тем самым аутентифицируя инициатора связи. Схема «логин/пароль» способна применяться в таких системах, но уже локально, для защиты приватного ключа конкретно выбранного участника сети.

Таковые системы крайне разнородны в своём проявлении и именно поэтому способны становиться альтернативой классическим сервисам связи. Так например, вполне реальным

является замена существующих мессенджеров, социальных сетей, форумов, распределённых хранилищ, цифровых валют и т.д. на приложения с безопасной линией связи типа «клиент-клиент». Таким образом, клиент-безопасные приложения становятся новыми платформами связи, более качественными в своём проявлении, чем классические альтернативы.

3.3. Тайные каналы связи

Секретные, тайные, эзотерические каналы связи — есть соединения, располагаемые в заведомо замкнутом, незащищённом, враждебном окружении и имеющие характеристики безопасной передачи информации. В отличие от определения [31, с.147], в нашем случаем под тайными каналами будут пониматься системы «неорганически вживляющиеся» в уже существующие сети. При этом анонимность, родственная скрытым сетям, не является базисом секретных каналов связи и, следовательно, может быть отброшена из-за ненадобности или по необходимости. Из такого краткого определения можно выделить две формы тайных каналов связи:

1. Первой формой тайных каналов связи можно считать 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 [32], поскольку субъект остаётся открытым, а объект продолжает быть закрытым (только вместо сокрытия информации, скрывается сам факт её существования). 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). Примером такого поведения может служить использование программ типа PGP [31, с.785][33] на форумах, мессенджерах, социальных сетях.

2. Второй формой тайных каналов связи можно считать абстрактную анонимную сеть (более подробно в разделе «Абстрактные анонимные сети»). Виртуальная маршрутизация абстрактных анонимных сетей имманентна, способна сводиться к передаче объекта внутри единого, сингулярного приложения, связывающего всех субъектов изнутри. Таким приложением является сервер (или группа серверов находящихся в сговоре), 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.

Таким образом, тайные каналы связи являются лишь производными от клиент-безопасных приложений (первая форма) и анонимных сетей (вторая форма). Как третий отдельный вид скрытых систем таковые сети считать не стоит. Но так или иначе, их анализ полезен по нескольким другим причинам: 1) тайные каналы связи, в отличие от анонимных сетей и клиент-безопасных приложений, не создают собственные связи, а встраиваются в уже существующие, при этом повышая уровень безопасности и анонимности первичных систем; 2) тайные каналы связи позволяют выделить класс абстрактных анонимных сетей из-за своей «паразитической» специфики существования в заведомо небезопасных линиях связи.

Тайные каналы связи, использующие стеганографию, всегда имеют некий контейнер, в который помещается истинное сообщение [32, с.8]. 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, битами исходного сообщения. Таким образом, если размер изображения (то есть, контейнера) будет равен 2MiB (без учёта метаданных), то максимальный размер исходного сообщения (в лучшем случае) не будет превышать 256KiB.

Использование стеганографии, вместе с криптографией, может помочь в случаях, когда имеется вероятность или возможность нахождения скрытого сообщения в контейнере за время меньшее, чем необходимое. 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 [31, с.720]. Это не является последовательным объединением, использованием методов, как это было описано выше, а скорее оказывается их слиянием, синтезом и 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 рекуррентно могут находиться и в других секретных каналах, либо анонимных сетях (по причине того, что тайные каналы могут быть воссозданы совершенно в любых системах и ситуациях), тем не менее, подобный подход является очень сомнительным (по причине избыточности накопленных слоёв шифрования), специфичным (по причине редкости практического использования) и затратным (по причине уменьшения производительности программ, уменьшения ёмкости контейнеров).

Из-за высоких накладных расходов (в частности описанных выше), в тайных каналах связи (как правило) не предполагается существование сервисов связи, присущих анонимным сетям, в том числе и в своей второй форме. Иными словами каждый получатель становится конечной точкой маршрута, а не возможным промежуточным субъектом, ретранслирующим информацию истинному субъекту с заранее известным, транспарентным открытым текстом.

4. Анализ сетевой анонимности

Термин «анонимность» представляет собой достаточно сложное и комплексное понятие, потому как таковое зависит от контекста. Так например, анонимность может предполагать собой использование псевдонимов при письме или живописи, использование масок с целью сокрытия лиц при законных и незаконных действиях, в благотворительности с отсутствием каких бы то ни было инициалов, в Интернете с целью сокрытия своего сетевого трафика и т.д. Чтобы дать более точное понимание анонимности, необходимым следствием

является сокращение способов использования данного термина. В нашей статье наиболее важной становится анонимность направленная на сетевые коммуникации.

Сетевая анонимность хоть и является более узким термином, или вернее сказать подмножеством термина «анонимность», но до сих пор остаётся комлексным понятием. Единственным отличием становится независимость от контекста, потому как контекстом становится сам факт сетевых коммуникаций как среды исследования. Это и позволяет конкретизировать анонимность и выявлять основные векторы её развития.

4.1. Формирование стадий анонимности

Потому как сетевая анонимность есть объект фрагментированный со стороны определений и терминологий, то можно предположить неоднородность и факт становления, развития в определённых этапах. Вкратце, анонимность действительно становится возможным трактовать как некую градацию, поэтапность, которой присуще шесть стадий, выявляющих процесс её формирования посредством фаз отрицаний и внутренних противоречий.

1. Первая стадия является исходной точкой анонимности, тезисом, монадой примитивно не представляющей анонимность, пустотой инициализирующей мощность анонимности[4] $|A| = 0$. Примером является существование только прямого, прямолинейного, примитивного соединения «клиент-клиент» между двумя одноранговыми субъектами, что равносильно их стазисному состоянию. По причине отсутствия промежуточных субъектов мощность доверия на данном этапе представляет минимально возможную величину.

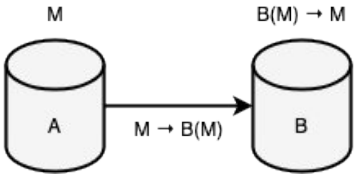

Рисунок 7. Первая стадия анонимности (прямое соединение)

2. Вторая стадия, становясь антитезисом, начинает отрицать первый этап, приводить систему к первичному метастазису, изменять собственным преобразованием способ

[4]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 $|A| = 1$ (вне зависимости от количества серверов). Нулевая мощность анонимности $|A| = 0$ возникает при существовании прямых соединений между субъектами (иными словами при отсутствии какой бы то ни было маршрутизации).

$$|A| = |Q(R)|,$$

где R - множество узлов участвующих в маршрутизации,
Q - функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами.

Так например, если $R = \{A, B, C\}$ — это множество узлов участвующих в маршрутизации, а подмножество $\{A, B\} \in R$ — кооперирующие узлы, то $Q(R) = [\{A, B\}, \{C\}]$ и, как следствие, $|A| = |Q(R)| = 2$.

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 повышаться до константного значения. Этап обеспечивает (инициализирует) 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 посредством сервера, что приводит их к фактическому разграничению, к взаимной анонимности и зависимости от общей платформы. В данной ситуации стоит заметить, что анонимность и безопасность идут вразрез друг с другом, противопоставляют себя друг другу, т.к. с одной стороны безопасность связи «клиент-клиент» становится скомпрометированной и дискредитированной, и в то же время, с другой стороны её же анонимность становится 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 убедиться далее. Описанную стадию вкратце именуют псевдо-анонимностью, а клиентов — анонимами.

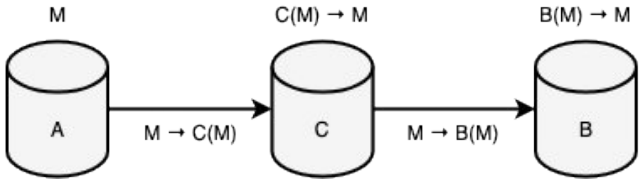

Рисунок 8. Вторая стадия анонимности (соединение посредством сервиса)

3. Третья стадия, являясь синтезом предыдущих стадий, 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 методом стремления к статичному значению $lim_{|A| \to C}$, где C — количество прокси-серверов. Данный метод предполагает выстраивание цепочки узлов, через которые будет проходить пакет. Мощность анонимности на данном этапе действительно повышается, но и 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. На *Рисунках 8, 9, 11, 12.* изображён абстрактный субъект @, способный быть как настоящим получателем, так и промежуточным субъектом — сервисом.

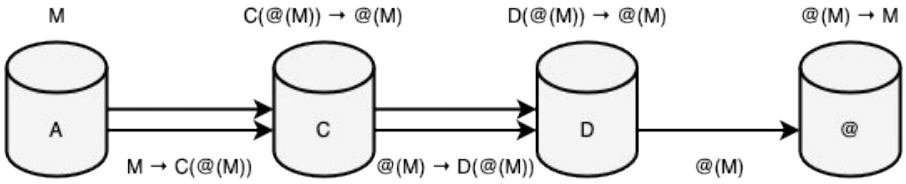

Рисунок 9. Третья стадия анонимности (Proxy транслирование)

4. Четвёртая стадия, как развитие третьего этапа, инициализирует способ изменчивости, множественного шифрования, полиморфизма информации посредством её

туннелирования. К такому этапу относятся VPN сервисы (виртуальные частные сети) как *N*-ое сочетание прокси-серверов со внутренними слоями шифрования [34], где мощность доверия и мощность анонимности эквивалентно третьей стадии. Отличительной особенностью четвёртого этапа является существование выходных узлов, постепенно «раскрывающих» истинный пакет, созданный до первичного туннелирования на отправляющей стороне, из-за чего и появляется возможность к сокрытию метаданных, связующих инициатора сообщения и сервер назначения. В связи с этим, данный этап изменяет способ маршрутизации, придаёт ему свойство полиморфизма как изменчивости закрытой информации по мере перехода от одного узла к другому, и отстраняет промежуточные узлы к анализу и сравниванию шифрованной информации. Таким методом скрывается настоящая связь между субъектами посредством их объекта, а следовательно и анонимат начинает обретать более истинный характер, при котором стремление системы к увеличению и сдерживанию мощности анонимности становится более качественным, в сравнении с третьей стадией.

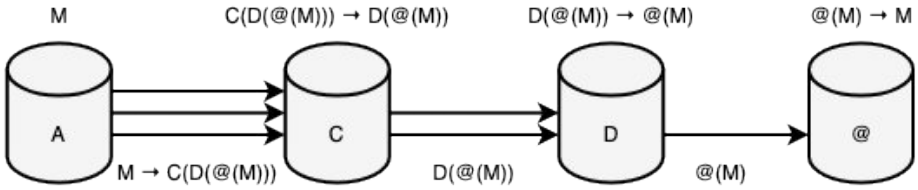

Рисунок 10. Четвёртая стадия анонимности (VPN туннелирование)

5. Пятая стадия, являясь синтезом первого этапа и отрицанием третьего, становится точкой окончательной замены сетевого адреса криптографическим, при которой идентификация субъектов отделяется от концепции сетевых протоколов, подчиняя узлы абстрактно-криптографической модели. Строятся платформы сетевой связи как базисы, поверх которых разрастаются криптографические соединения, инкапсулируя взаимодействия субъектов со своим основанием. Именно на данном этапе мощность доверия вновь становится минимально возможной величиной, а потому и все приложения построенные на пятой 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) и т.д. [35][36], где главным фактором идентификации клиентов становятся криптографические адреса (публичные ключи, хеши публичных ключей). Сеть начинает представлять собой не только гибридный, но и одноранговый характер поведения узлов с возможным и дополнительным динамическим способом определения мощности анонимности, как $0 < |A| \leq N$, где N — количество узлов в сети, обуславливаемым слепой, заливочной маршрутизацией [4, с.398] и криптографической идентификацией. При этом, стоит заметить, что на данном этапе не существует какого бы то ни было полиморфизма информации (как это было в четвёртой стадии), что приводит к внутренним противоречиям одновременного прогресса и регресса анонимности. Поэтому пятую стадию можно вкратце охарактеризовать игнорированием анонимности (экзотеричностью) со стороны субъекта и её сохранением (эзотеричностью) в передаваемом объекте. На *Рисунок 11.* под сетью понимается переключение системы из состояния сетевой идентификации к идентификации криптографической, вследствие чего происходит абстрагирование информации об отправителе для получателя и о получателе для отправителя непосредственно.

Рисунок 11. Пятая стадия анонимности (соединение посредством абстрактной сети)

6. Шестая стадия приводит к единовременному отрицанию и синтезу четвёртой стадии, как системы неориентированной на анонимную идентификацию субъектов, и пятой стадии, как системы ненаправленной на анонимную связь между субъектами. В такой синергии объединяются свойства полиморфизма (анонимное связывание) и криптографической идентификации (анонимное определение), что приводит не только к анонимату отправителя информации, но и к обезличиванию получателя, вследствие чего определение анонимности становится более качественным и цельным. Мощность анонимности на данном этапе становится эквивалентно четвёртому этапу, равно как и мощность доверия (причина ухудшения мощности доверия относительно пятой стадии приведена в разделе «Проблематика безопасности анонимных сетей»). Примером шестой стадии является большинство скрытых сетей, наподобие Tor (onion routing) [37], I2P (garlic routing) [38], Mixminion (mix network) [39] и т.д. На *Рисунок 12.* изображён прототип функционирования системы Tor с запросом ориентированным на внутренний ресурс (в качестве упрощения показана схема с двумя промежуточными узлами).

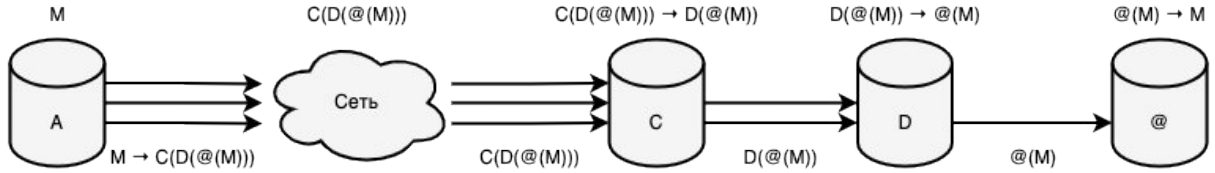

Рисунок 12. Шестая стадия анонимности (абстрактная сеть + туннелирование)

Стоит заметить, что четвёртая и пятая стадии появляются параллельно друг другу, что приводит к сложности (а скорее даже к невозможности) точного опознавания и определения последовательности развития анонимности в целом. Такой порядок стадий был взят по количеству качественных изменений. Так например, в четвёртой стадии (относительно третьей) был добавлен только полиморфизм информации, в то время как в пятой стадии была уменьшена мощность доверия, появилась криптографическая идентификация, возник новый способ маршрутизации и вернулась поддержка одноранговых соединений. С другой стороны, пятая стадия также справедливо могла стать четвёртой, базируясь не на развитии анонимности субъектов, а на развитии безопасности объектов. В таком случае, пятый этап являлся бы финальной формой, в то время как текущая четвёртая стадия не проектировалась бы вовсе.

Также стоит отметить, что вторая и пятая стадии анонимности характеризуются имплозивным характером поведения информации в степени большей, чем все остальные стадии, потому как первые предполагают не только метод распространения объектов, но также и способность их сдерживания для последующего извлечения и потребления. Такие стадии именуются платформами связи, т.к. сама коммуникация между субъектами начинает обеспечиваться не только поточным транспортированием объектов (как самого факта

передачи), но и «подгрузкой», посредством промежуточных субъектов, ранее сохранённых объектов, в основании которых уже содержится информация об отправителе и/или получателе. Другие же стадии абстрагируются от конечного потребителя информации и акцентируют внимание только на сам способ передачи. Исключением всего вышесказанного является лишь первая стадия анонимности, где сам факт передачи является одновременно и способом финального получения информации.

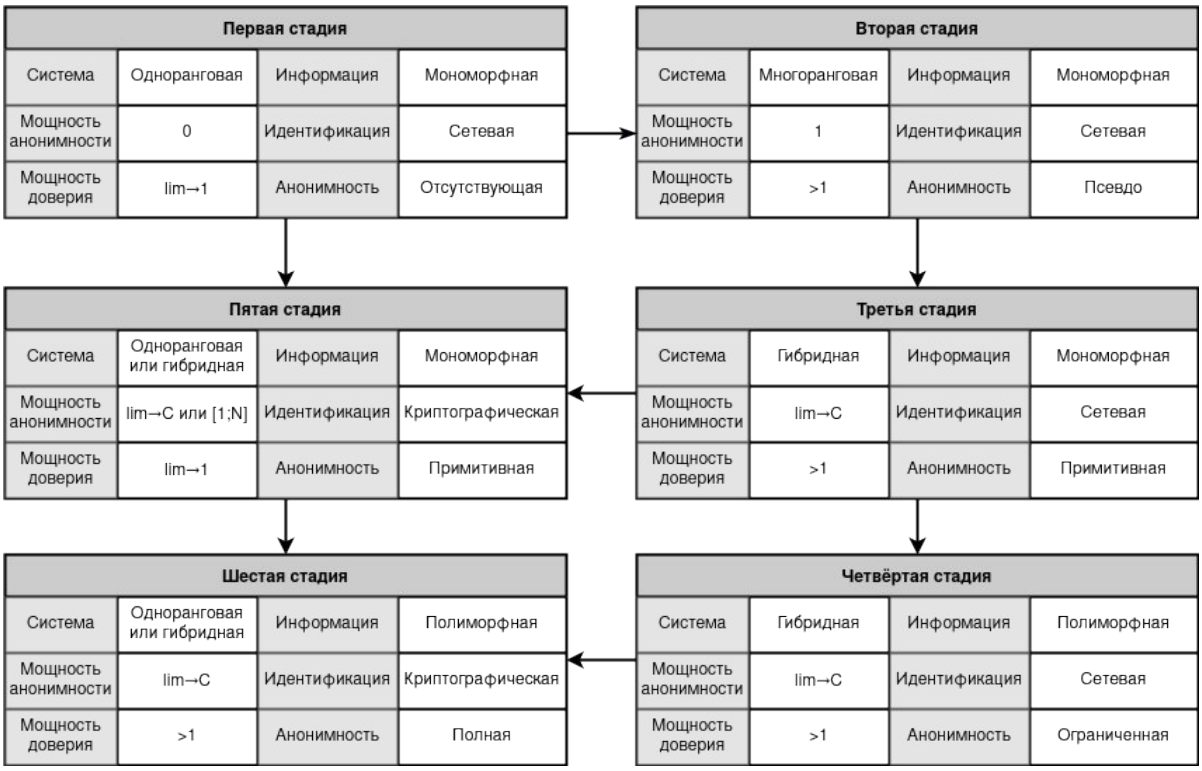

Рисунок 13. Развитие анонимности как процесс формирования стадий

Защита, определяемая связью «клиент-клиент», зарождается на моменте первой стадии анонимности и в последствии сразу же заменяется клиент-серверным шифрованием второго этапа. Такая быстрая подмена и разложение прямой коммуникации на платформу связи обусловлена неспособностью и ограниченностью первой стадии к эксплозии, расширению сетевых «границ», при которой субъекты не способны массово связываться без создания промежуточных узлов. Последующее и более качественное возрождение безопасной «клиент-клиент» коммуникации, убирающее ограничение в расширении, появляется на пятом этапе и ровно там же заканчивается, потому как целью всех последующих стадий уже является сокрытие субъектов информации посредством методов транспортирования объекта на базе криптографических адресов, где более не ставится вопрос истинности принимающей стороны.

Главным достоинством пятой стадии анонимности является возможность к идентификации субъектов в одноранговых и гибридных системах на основании криптографических методов, что ведёт к целостности, а также к аутентификации передаваемой информации, не зависимой от сторонних узлов и серверов [40, с.223]. Дополнительно может появляться свойство конфиденциальности, где информация начинает представлять собой суть секретного, тайного, шифрованного, а не открытого и общего объекта. Но и само свойство конфиденциальности на данном этапе — есть дополнительный критерий, а следовательно, может быть удалён, если таковой является избыточным для самой

системы. Как пример, в криптовалютах имеются свойства целостности и аутентификации, но не всегда конфиденциальности.

На основе пятой стадии анонимности становится возможным формирование тайных каналов связи первой формы как это представлено на *Рисунок 14*. Такое свойство достигается появлением криптографической идентификации субъектов, благодаря которому становится возможным абстрагироваться от сетевой идентификации.

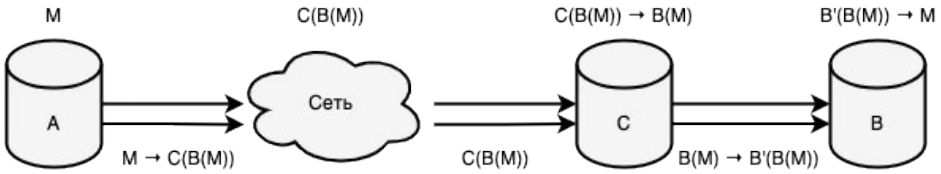

Рисунок 14. Тайный канал связи на базе пятой стадии анонимности, где *A, B* – отправитель / получатель, *C* – сервис связи

На основе определённых подмножеств пятой и шестой стадий анонимности (более подробно в разделе «Абстрактные анонимные сети») становится возможным формирование тайных каналов связи второй формы.

Таким образом, тайные каналы связи в общих своих свойствах полностью абстрагируются от первичной сети, выстраивают собственные способы коммуникаций и начинают базироваться на пятой или шестой стадии анонимности.

Из всего вышесказанного можно вывести основные критерии (пункты) анонимности на базе которых будет доступно формирование анонимных сетей с повышенным уровнем безопасности (полные скрытые системы).

1. Анонимность обязана быть внутренней, относительно анализа со стороны узлов, и внешней, относительно анализа трафика сети. Данный критерий должен обуславливаться разрывом связи между субъектами посредством их объекта на основании запутывающего алгоритма маршрутизации.

2. Анонимность обязана быть двунаправленной относительно субъектов информации и применяться как к отправителю — инициатору связи, так и к получателю — платформе связи или конечному адресату. Данный критерий должен обуславливаться разрывом связи между идентификацией сетевой и криптографической.

3. Анонимность обязана предотвращать сохранение данных и метаданных в транспарентном состоянии для промежуточных узлов. Данный критерий должен обуславливаться заменой всех платформ связи пятой стадией анонимности, тем самым уменьшая мощность доверия до теоретически возможного минимума.

Скрытая система наделённая только первыми двумя пунктами является анонимной сетью и принадлежит либо пятой^ (более подробно в разделе «Абстрактные анонимные сети»), либо шестой стадии анонимности. Скрытая система наделённая только последними двумя пунктами является клиент-безопасным приложением и принадлежит исключительно пятой стадии анонимности. Скрытая система надёланная сразу тремя критериями анонимности является полной и принадлежит не отдельной стадии анонимности, а их комбинациям (более подробно в подразделе «Проблематика безопасности анонимных

сетей»). Система наделённая только одним пунктом из трёх не является скрытой. Под системой с первым пунктом может пониматься VPN туннелирование (четвёртая стадия анонимности), а под вторым – сервисы связи (вторая стадия анонимности). Не существует систем исключительно с третьим пунктом, ровно как и комбинации третьего пункта с первым (исключая второй). Связано это с тем, что третий критерий является следствием второго (обратное суждение неверно). Все вышеприведённые дескрипции можно представить в более кратком описании:

1. Выстроенная «цепочка» VPN сервисов ∈ первый пункт
2. Централизованные сервисы связи ∈ второй пункт
3. Анонимные сети = первый пункт ∩ второй пункт
4. Клиент-безопасные приложения = второй пункт ∩ третий пункт
5. Полные скрытые системы = первый пункт ∩ второй пункт ∩ третий пункт

Таким образом, на основании вышеприведённых критериев можно выявить базовое определение анонимности относительно общего вида скрытых систем, где под сетевой анонимностью будет пониматься разрыв большинства логических связей между транспортируемым / хранимым объектом и его субъектами, а также между сетевой и криптографической идентификациями.

4.2. Двойственность первой стадии анонимности

При начальном рассмотрении первой стадии анонимности выражается простейшая форма, инициализирующая развитие анонимата, при которой прямолинейность соединений создаёт примитивность её организации. Но при дальнейшем и более детальном анализе анонимных сетей можно заметить исключительно противоречивое свойство первой стадии анонимности, сперва исключающее, а при пересмотре образующее теоретически абсолютную анонимность в свойственной прямолинейности субъектов. Данное качество возникает при генерации объекта способного скрывать всю информацию о субъекте, включая и сам факт своей передачи и своего хранения. В подобной системе не существует никакой криптографической идентификации (что исключает все стадии выше четвёртой) и условно маршрутизации (что исключает все стадии выше первой). На основе таких качеств выявляется три парадокса.

1. Первая стадия анонимности исключает из своего рассмотрения промежуточные субъекты. Если данная стадия переходит в состояние анонимной сети, то внутри неё способны зарождаться сервисы связи, основанные либо на второй, либо на пятой стадиях анонимности. Таким образом, получатель в анонимной сети становится не равен конечному получателю, что противоречит определению первой стадии анонимности.

2. Мощность доверия в первой стадии анонимности имеет минимально возможную величину. Если данная стадия переходит в состояние анонимной сети, то внутри неё способны зарождаться сервисы связи, основанные на второй стадии анонимности. Таким образом, появляются промежуточные узлы исполняющие роль конечных получателей, что приводит к повышению мощности доверия и как следствие противоречит определению первой стадии анонимности.

3. Мощность доверия в первой стадии анонимности имеет минимально возможную величину. При исключении промежуточных узлов, мощность доверия не уменьшается, потому как проблема переходит на плоскость множества конечных получателей (т.к. анонимность базируется только на широковещательной открытой связи без сокрытия информации от третьих лиц), что противоречит определению первой стадии анонимности.

Все парадоксы базируются на самой двойственной форме первой стадии, когда таковая одновременно вбирает в себя и выраженное транспортирование объекта, и конечное его хранение. Парадоксы своим существованием фактически расщепляют двойственность и образуют новое подмножество, как неявную градацию первой стадии анонимности. Во всех последующих упоминаниях вышеописанный этап с присущими парадоксами будет отображаться как «первая^ стадия анонимности», со знаком циркумфлекса. В качестве примера существования первой^ стадии анонимности выделяют скрытые сети базируемые на проблеме обедающих криптографов [41] (DC-сети), такие, как Dissent [42] и Herbivore [43]. Чистая форма первой^ стадии анонимности приводит к следующим недостаткам.

1. Масштабируемость. Первая^ стадия анонимности приводит к необходимости выстраивания большого количества прямых соединений, что приводит к проблеме масштабируемости, где каждый новый пользователь обязан подключаться ко всем существующим участникам сети. Проблема решается переводом первой^ стадии анонимности на градации высшего порядка, образуя промежуточные узлы полностью не влияющие на уровень анониности в сети. Dissent переводит систему на третью стадию анонимности, Herbivore на третью при локальной топологии и на пятую при глобальной.

2. Коллизии. В один период времени может существовать только один отправитель сообщения. При параллельной генерации сообщений двумя и более участниками сети происходит коллизия, приводящая к наложению информации. В большей части исследований проблема решается выставлением расписания генерации сообщений, что приводит к обязательной последовательности. Для схем подобного рода в Dissent используются перемешивания, а в Herbivore малые группы.

3. Чистая анонимность. В исходном виде анонимность первой^ стадии идёт в полном отрыве от безопасности передаваемого объекта, где распространение информации происходит только на основе широковещательного соединения, при котором получателем сообщения является вся система. Для обеспечивания безопасной линии связи от отправителя до единственного получателя (истинного или промежуточного) должен происходить переход первой^ стадии анонимности на пятую градацию в концепции тайного канала связи.

Таким образом, первая^ стадия анонимности, как чистая форма выражения анонимата, является неприменимой в современных реалиях из-за критичных недостатков, что приводит к необходимости комбинировать данную стадию с градациями высшего порядка. Также можно выявить интересную закономерность, которая разделяет первую стадию анонимности на два вектора развития — на доказуемую безопасность объектов без анонимности субъектов (классическая первая стадия) и доказуемую анонимность субъектов без безопасности объектов (первая стадия с парадоксами или неклассическая форма).

Первый вектор базируется на безопасности объектов, вследствие чего, становится возможным последующий полиморфизм информации, как метод построения запутывающей маршрутизации. Второй вектор базируется на анонимности субъектов, вследствие чего,

становится необходимым совмещение с тайным каналом связи, как методом нацеленным на обеспечение безопасности объектов. Оба вектора в конечном счёте сводятся в точке анонимности субъектов с приемлемым уровнем безопасности объектов на основе криптографической идентификации, как это изображено на *Рисунок 15*.

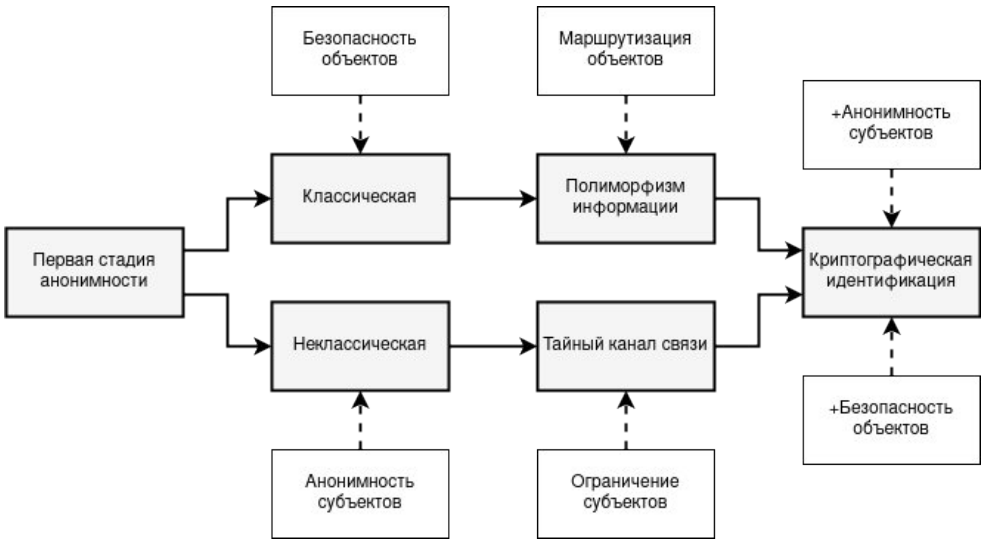

Рисунок 15. Двойственный вектор развития скрытых сетей относительно первой стадии анонимности

В завершение данного раздела стоит заметить одну важную составляющую. Первая^ стадия анонимности, поначалу, словно не имеет никакой маршрутизации, что явным образом противоречит термину «анонимная сеть». Существование тайного канала связи никак не изменяет картину, потому как он внедряется в уже готовую систему и, как следствие, оставляет мощность анонимности на прежнем, первоначальном уровне. Тем не менее маршрутизация, хоть и специфичная, но существует в первой^ стадии. Это можно доказать тем фактом, что участники такой сети кооперируют и объединяют информацию в одну выходную последовательность бит, где даже при связи «*все-ко-всем*» передаётся уже «скрещиваемая» информация. Если информация в процессе своеобразной маршрутизации претерпевает изменения от одного узла к другому, то это представляет форму полиморфизма информации. Таким образом, развитие анонимных сетей на базе DC-сетей является лишь инверсивным способом применения основных конструктов «анонимности субъектов» и «безопасности объектов», относительно классической формы первой стадии анонимности, а значит приводит к равенству «первая^ стадия анонимности + тайный канал связи = шестая стадия анонимности».

4.3. Проблематика безопасности анонимных сетей

При существовании и полной реализации, а также доступности скрытых сетей, проблема, связанная с мощностью доверия, возвращается. Это кажется парадоксальным, ведь сама задача ещё решилась на пятой стадии анонимности, когда мощность доверия становилась минимально возможной величиной. Сложность заключается именно в том, что при достижении 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 доминирующее состояние. Таким образом, осуществляется трансфузия двух свойств, где анонимные сети

начинают инициироваться противоположным, инволютивным действием к пятой стадии анонимности, а именно — игнорированием анонимности (экзотеричностью) со стороны передаваемого объекта и её сохранением (эзотеричностью) в субъекте.

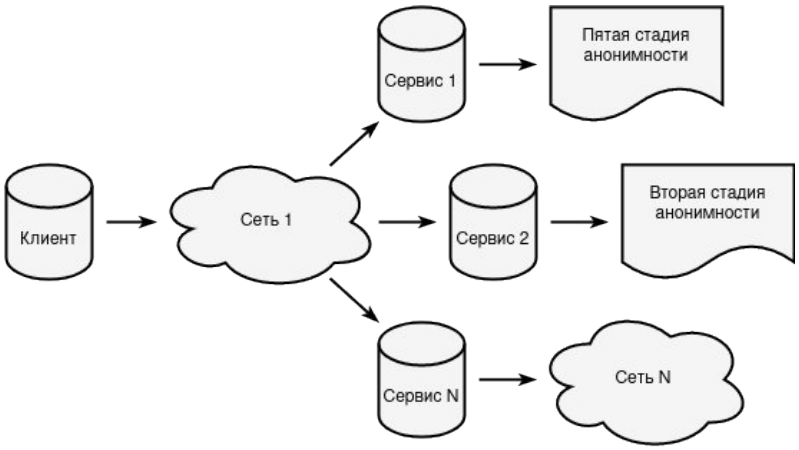

Рисунок 16. Взаимодействие скрытых сетей со внутренними сервисами

Сутью проблемы является возможность создания сервисов внутри скрытых сетей не основанных на пятой стадии анонимности (*Рисунок 16*), что приводит к возникновению приложений на базе второй стадии, представляющих угрозу информационной безопасности. Это связано с тем фактом, что анонимные сети в массе своей являются лишь способом маршрутизации к конечному субъекту, представляют собой некую платформу сервисов и позволяют размещать внутри себя 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 в 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.

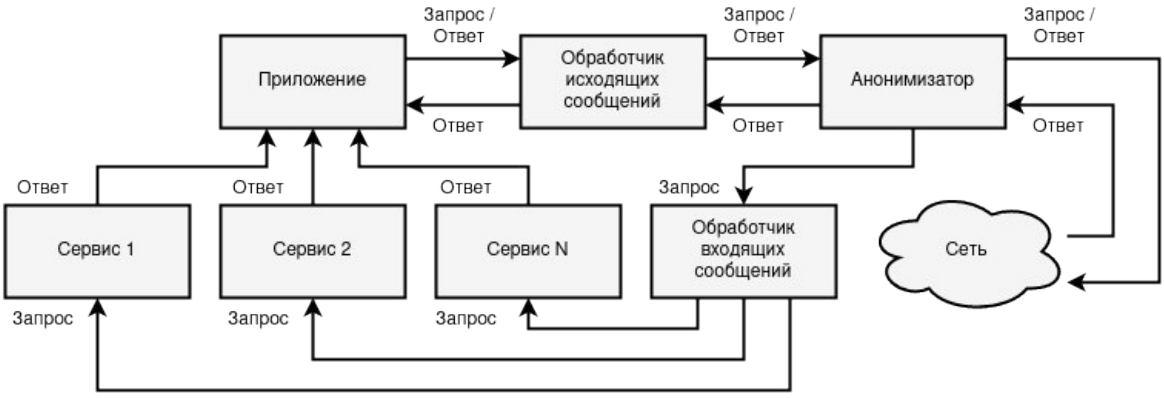

Рисунок 17. Пример архитектуры приложения анонимной сети с несколькими принимающими сервисами

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 пятой стадии анонимности. Доступ к любым другим сервисам, не имеющих пятую 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. Примером таких сочетаний могут служить связи Tor+Bitcoin, I2P+Filetopia и т.п., или более монолитные технологии Monero [44], Dash [45] и т.д. Только на данном основании скрытые системы становятся полными.

5. Абстрактные анонимные сети

Среди анонимных сетей можно выявить класс систем с теоретически доказуемой анонимностью и максимально разграничивающим свойством, приводящим к наибольшему разрыву связей между объектом (как информации) и его субъектами (в лице отправителя и получателя). Из-за своей специфичной архитектуры передача информации может осуществляться в любой дуплексной среде вне зависимости от расположения и связей узлов, что полностью отрывает распространение объектов от своей сетевой архитектуры и переводит маршрутизацию в этап виртуального транслирования. За счёт такого свойства данные сети могут быть использованы в построении тайных каналов связи второй формы. Анонимные сети, с вышеописанными характеристиками, будут именоваться абстрактными.

Рисунок 18. Абстрактные анонимные сети являются подмножеством класса теоретически доказуемой анонимности

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

5.1. Модель на базе очередей

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

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

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

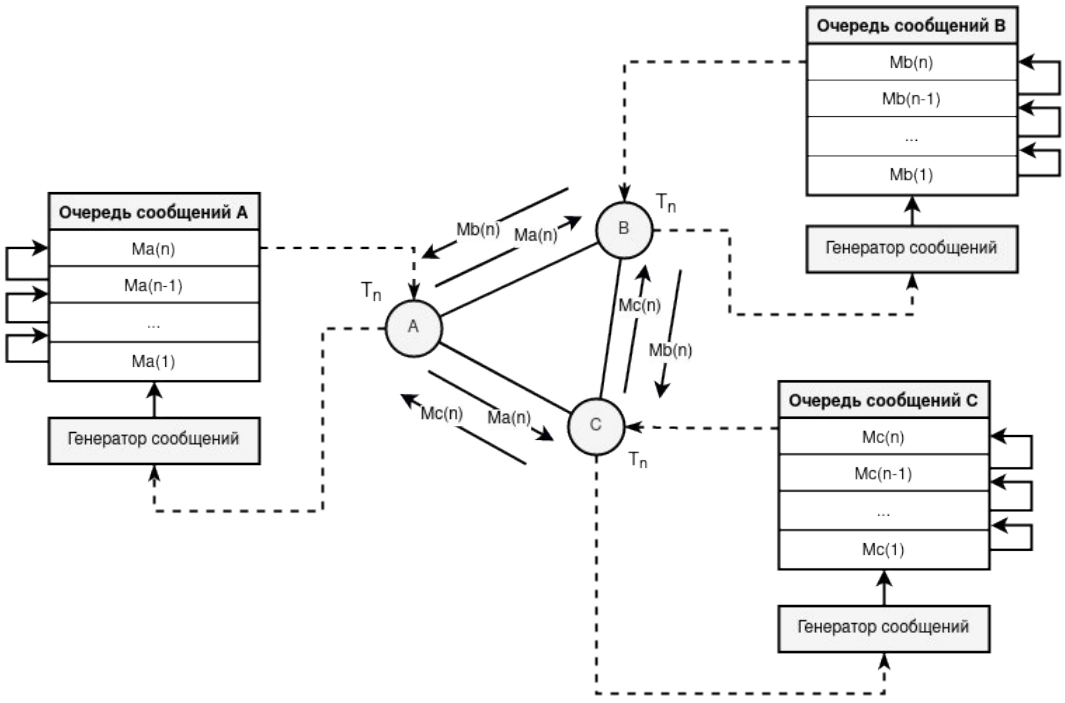

Рисунок 19. Схема абстрактной анонимной сети на базе очередей со стороны внешнего наблюдателя

Предположим далее, что необходимо защититься от q-ого количества внутренних наблюдателей системы из количества $q+|\{A, B, C\}|$ узлов, где известно, что узел C – не связанный в сговоре маршрутизатор для одного из узлов A или B. Целью атакующего становится сопоставление факта отправления ответа из множества $\{A, B\}$ с конкретным его элементом. В идеальной системе (теоретически доказуемой) вероятность обнаружения ответа составит 1/2. При существовании N узлов несвязанных между собой общими целями и интересами, вероятность становится равной $1/N$. Итоговая система должна удовлетворять данным свойствам.

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

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

1. Каждый субъект сети должен выстроить период генерации пакета равный T_n, где $n \in Q$, n – величина периода, не менее и не более. Иначе становится эффективна атака со стороны внутреннего наблюдателя. Несогласованность константного числа T_n с другими участниками сети приведёт к возможности разграничения субъектов по подмножествам с разными периодами генераций.

2. Каждый субъект сети выстраивает период равный T_n полностью локально, без кооперирования с другими субъектами сети. Это условие является лишь упрощением системы, само кооперирование не приведёт к нарушению протокола, потому как предполагается, что сама генерация пакетов, а конкретно время генерации, не является секретом.

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

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

5. Каждое сообщение зашифровывается монолитным криптографическим протоколом с множественным туннелирование и проходит сквозь маршрутизирующие узлы (более подробно в разделе «Монолитный криптографический протокол»). Такое свойство приведёт к сильному разрыву связей между объектом и его субъектами, а также между идентификацией сетевой и криптографической.

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

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

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

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

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

Явным недостатком данной архитектуры становится подверженность атакам отказа в обслуживании (DDoS), как для конкретного субъекта, перегружая его очередь сообщениями, так и для всей сети. Связано это с тем, что в основе системы используются очереди, сохранающие и накапливающие сообщения, а также слепая маршрутизация, порождающая наибольшую несвязанность объекта с его субъектами за счёт полного распространения информации по всем участникам сети.

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

Тем не менее в выстроенной системе становится достаточно легко доказать невозможность атаки со стороны внешнего наблюдателя, анализирующего дифферентность сети. Если каждый субъект соблюдает генерацию пакета по локальному периоду (даже гипотетически с разными значениями T_n), то становится невозможным установление факта отправления, получения, маршрутизации или ложной генерации, потому как наблюдатель, в конечном счёте, способен лишь видеть определённые шифрованные сообщения

генерируемые каждый промежуток времени равный T_n. Также, если внешним наблюдателем будут блокироваться определённые субъекты информации, кардинально данный подход ситуации не изменит.

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

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

a) Частный случай. Предположим, что существует крайне стабильная система при которой каждый узел из множества {*A, B, C*} выставил в один и тот же промежуток времени значение равное T_n без отставания по времени относительно всех остальных участников сети. Все участники генерируют запрос секунда в секунду каждые T_{ni} по периоду. Предположим, что $T_n = 3$, тогда генерацию можно представить в виде *Таблицы 2*.

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

Таблица 2. Стабильная система со множеством участников {*A, B, C*} и $T_n = 3$

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

Теперь предположим, что маршрутизация субъекта C существует. Если внутренний наблюдатель хочет раскрыть субъектов {*A, B*}, то можно предположить, что ему необходимо каким-либо образом обойти ретрансляцию субъекта *C*. Но исключить узел *C* из сети не

является решением, потому как прекратится вся последующая связь с субъектом A или B. Другим способом расскрытия (и куда более продуктивным) является уже исключение одного субъекта из множества $\{A, B\}$, иными словами заблокировать участника сети на определённый период времени mT_n. Тогда в таком случае активный внешний наблюдатель блокирует одного из субъектов $\{A, B\}$, после этого активный внутренний наблюдатель посылает запрос на одного из субъектов множества $\{A, B\}$. Если отправитель получает ответ, значит истинным получателем информации является не исключённый участник, в противном случае – исключённый.

Для предотвращения активных атак со стороны сговора внешних и внутренних наблюдателей необходимо добавить дополнительный (но не единственно возможный) 11_1 пункт, который представляет новую псевдо роль субъектов в качестве контролирующих узлов. Такая атака приводит к невозможности деанонимизации субъектов посредством частичного блокирования, потому как её следствием станет взаимоблокировка субъектов. Тем не менее добавление данного пункта скажется на том, что сама сеть выйдет из класса абстрактных анонимных сетей, потому как добавится необходимость в поточном распространении информации.

11_1. Каждый действующий субъект сети выставляет минимум одного существующего пользователя в роли контролирующего узла для предотвращения от активных атак методом исключения участников системы. Суть такого пользователя в понимании его существования. Если связь с подобным субъектом будет разорвана, то все последующие действия автоматически прекращаются. Само соединение функционирует за пределами механизма очередей, что, тем не менее, не приводит к снижению уровня анонимности, потому как все субъекты начинают подчиняться этому правилу однонаправленно (в такой концепции не существует функций типа запрос/ответ, существуют только поточные уведомления своего присутствия).

Хоть теоретически сама атака становится невозможной, но в практическом смысле и в долгосрочном наблюдении она более чем реальна. Связано это с тем, что одноранговая архитектура как таковая приводит к постоянному и динамичному изменению связей между субъектами. Это в свою очередь может приводить к исключениям групп субъектов связанных контролирующими узлами, потому как последние обязаны быть действующими и настоящими участниками системы.

Ещё одним возможным решением вышеописанной проблемы может стать использование доверенных соединений среди участников сети. Такой подход ограничивает действия активных внутренних наблюдателей и за счёт данного свойства позволяет снизить риски деанонимизации, а также сохранить абстрактность системы (по сравнению с пунктом 11_1).

11_2. Каждый действующий субъект сети выстраивает связи с другими участниками, основываясь на субъективности к уровню доверия, устанавливая и редактируя белый список на своей стороне. Чтобы успешно подключиться к сети такого рода, субъекту необходимо стать доверенным узлом, то есть пользователем, которому кто-либо доверяет. Сложность исполнения атаки на подобную сеть будет сводиться к сложности встраивания подчиняемых узлов, потому как каждый получатель информации, в конечном итоге, должен будет заранее устанавливать список возможных отправителей.

Сети с таким свойством именуются friend-to-friend (F2F) сетями [46]. Естественным недостатком является малая экспансия, как возможность масштабирования системы. С другой стороны, как раз такое качество позволяет дополнительно (и довольно эффективно) сдерживать недостатки самой структуры, когда увеличивающееся количество субъектов приводит к регрессу производительности системы. В общем представлении такой метод защиты достаточно эффективен против внутренних активных наблюдателей (особенно с практической точки зрения), но теоретически является более сложной моделью. Анонимность такого случая начинает базироваться на гипотетически большем количестве связей между участниками, чем при выстраивании константно заданного количества маршрутизирущих узлов, что и приводит к дополнительным рискам деанонимизации субъектов.

Также ещё одним возможным решением может стать синтез подходов, что закономерно объединит не только положительные, но и отрицательные стороны этапов 11_1 и 11_2. В следствии такого соединения система перестанет быть абстрактной (за счёт необходимости в поточном поддержании соединений), появится свойство малой экспансии (за счёт принадлежности к F2F-сети) и увеличится сложность практической реализации (за счёт, соответственно, синтеза двух подходов). Тем не менее, теоретическая безопасность выйдет на более лучший уровень, потому как если один из доверенных субъектов станет скомпрометированным, то останется дополнительный слой защиты в лице маршрутизаторов.

b) Общий случай. Предположим, что существует нестабильная система при которой каждый узел из множества {*A, B, C*} выставил в разный промежуток времени значение равное T_n с отставанием по времени относительно всех остальных участников сети. Все участники генерируют запрос в разные секунды, но также сохраняя локальный период равный T_n. Предположим, что $T_n = 3$, тогда генерацию можно представить в виде *Таблиц 3, 4, 5* относительно расположения субъекта *C* к другим участникам.

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

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

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

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

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

Таблица 5. Нестабильная система со множеством участников {*A, B, C*} и $T_n = 3$, где узел *C* находится в конце генерации

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

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

Предотвращением атаки является отправление истинного пакета на вторую итерацию периода маршрутизирующей стороны (относительно текущего времени). Теперь репродуцируем вышеописанную атаку на систему с таким условием. Также предположим, что сетью является система на базе *Таблицы 3*. Если атакующий сгенерирует сообщение в момент времени T_{n1}, то получит ответ только в момент T_{n3-2}. Получателем в такой системе может оказаться любой из множества {*A, B*}, потому как ответ может быть отправлен как в момент времени T_{n2-1} (субъект *A*), так и в T_{n2} (субъект *B*). Чтобы субъект *B* отправил ответ именно в T_{n2}, то перед ним он помещает в очередь ложное сообщение, тем самым отодвигая отправление истинного сообщения по сети на одну итерацию. Аналогичные ситуации распространяются и на *Таблицы 3, 4*.

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

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

1. Исчезнет необходимость в промежуточных узлах и кооперировании с ними для установления периодов. Как следствие, не будет надобности в условностях отправления сообщений на конкретной итерации периода маршрутизирующего узла.

2. Исчезнет необходимость в использовании механизмов несвязываемости размеров сообщений (подробнее в подразделе «Противодействие обнаружению динамики размерности пакетов» раздела «Монолитный криптографический протокол»).

3. Исчезнет необходимость в анализе частного и общего случаев, потому как таковые являются следствием существования маршрутизирующих узлов и полиморфизма информации. И как следствие, пункт 3 заменится пунктом 11_2.

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

Теоретически основным отличием таковых подходов становятся иные векторы нападения, где при алгоритме «очередь» атаки начинают принадлежать способам компрометации доверенных узлов, а при алгоритме «очередь+полиморфизм» – компрометациям маршрутизирующих узлов. В обоих случаях требуется сговор скомпрометированного узла с внешним глобальным наблюдателем. При удовлетворении условия нескомпромитированности ключевых субъектов, анонимность двух алгоритмов будет удерживаться на определённо заданном уровне.

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

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

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

Также, из-за специфичности очередей, сети такого рода не могут выстраивать сильную концентрацию любых сервисов связи, потому как запрос-ответ со стороны разных субъектов становится единым последовательным действием из-за чего становится невозможным эффективно создавать общий сервис на множество клиентов в один промежуток времени. Как пример, пятая^ стадия анонимности на базе очередей может эффективно быть применима при построении мессенджеров, с неотслеживаемостью факта переписки (дополнительно с E2E-шифрованием), но не может использоваться при построении файловых-сервисов расчитанных на множество клиентов. Если существует N-ое количество субъектов взаимодействующих с файловым-сервисом в один промежуток времени и каждый пытается скачать файл размером в X, то при размере пакета в Y (где $X > Y$) с конфигурационным периодом равным T_n все участники гарантированно смогут скачать данный файл только спустя $M = T_n N \lceil X/Y \rceil$. При увеличении N, конечная скорость скачивания будет линейно регрессировать, при уменьшении T_n будет производиться большое количество спама, при котором стабильность работы узлов станет уменьшаться, при увеличении Y очередь будет содержать меньшее количество объектов, тем самым приводя к игнорированию большого количества запросов от клиентов. Таким образом, эффективность использования пятой^ стадии анонимности на базе очередей зависит от конкретных типов задач.

5.2. Модель на базе увеличения энтропии

Другой абстрактной анонимной сетью может быть система на базе увеличения энтропии. Со стороны теоретического доказательства анонимности она более трудоёмкая и

в некой степени более «хрупкая» (чем сеть на основе очередей), потому как большинство действий сводит к вероятностям конкретно выбранного субъекта, а не к действиям всей группы. Чтобы правильно доказать существование теоретической анонимности в таких условиях – необходимо рассматривать факт связывания субъектов между собой, анализируя при этом постоянный прирост энтропии.

Предположим, что существует всего три узла {*A, B, C*} и сама сеть работает по принципу вероятностного полиморфизма, где каждый субъект может с вероятностью 1/2 выстроить маршрут с промежуточным узлом или без него соответственно. В конечном итоге будет образовано два разных и равновероятно возможных действия.

1. При полиморфизме информации будет существовать три этапа транспортирования информации: (*A → B ИЛИ A → C*) → (*B → C ИЛИ C → B*) → (*B → A ИЛИ C → A*)[5].

2. При отсутствии полиморфизма информации будет существовать всего два этапа транспортирования информации: (*A → B ИЛИ A → C*) → (*B → A ИЛИ C → A*).

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

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

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 минимальной константе *k = 2*, которую можно свести к следующему 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 начинают трактоваться двумя полностью самодостаточными процессами: запрос(1) - ответ(1) - запрос(2) - ответ(2) или запрос(1) - маршрутизация(1) - маршрутизация(~1) - ответ(1), что в свою очередь 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 таком случае, является лишь запрос(1), созданный генезис-инициатором связи, который будет трактоваться всегда детерминировано. Но и здесь, в первую очередь, стоит заметить, что при последующих запросах данная проблема

[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.

всегда будет угасать из-за увеличивающейся энтропии [47], приводящей к хаотичности действий посредством метаморфозов вероятностного полиморфизма. Так например, на следующем шаге появится неопределённость вида запрос(3) = запрос(2) = маршрутизация(~2), означающая неоднозначность выявления отправителя. Итоговую модель можно представить следующим способом:

Метаморфозы вероятностного полиморфизма	Расширение энтропии
1. (*A → B ИЛИ A → C*) [# *A* - инициатор] [# *B или C* - получатель или маршрутизатор]	1, 2. [запрос(1)] → | 0 бит |
2. (*B → C ИЛИ C → B*) [# *B или C* - маршрутизатор] *ИЛИ* (*B → A ИЛИ C → A*) [# *A* - инициатор] [# *B или C* - получатель]	1. [маршрутизация(1)] = 2. [ответ(1)] → | 1 бит |
3. (*B → C ИЛИ C → B*) [# *B или C* - маршрутизатор] *ИЛИ* (*B → A ИЛИ B → C*) [# *B* - инициатор] [# *A или C* - получатель или маршрутизатор]	1. [маршрутизация(~1)] = 2, 3. [запрос(2)] → | 1 бит |
4. (*B → A ИЛИ C → A*) [# *A* - инициатор] [# *B или C* - получатель] *ИЛИ* (*A → B ИЛИ C → B*) [# *B* - инициатор] [# *A или C* - получатель] *ИЛИ* (*A → C ИЛИ C → A*) [# *A или C* - маршрутизатор]	1. [ответ(1)] = 2. [ответ(2)] = 3. [маршрутизация(2)] → | 2 бита |
5. …	…

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

При этом, стоит заметить, что в сети на базе увеличения энтропии, на уровне ядра, заложен механизм постоянного умножения, увеличения энтропии, как это представлено на *Рисунке 20*, вследствие чего зарождаются и усваиваются одни лишь ложные логические суждения (что будет показано далее). Если таковые суждения априори представляют ложные выводы на любые выражения, то это эквивалентно полному доминированию энтропии над системой, в которой становится невозможным выявление закономерностей посредством декомпозиции её составляющих.

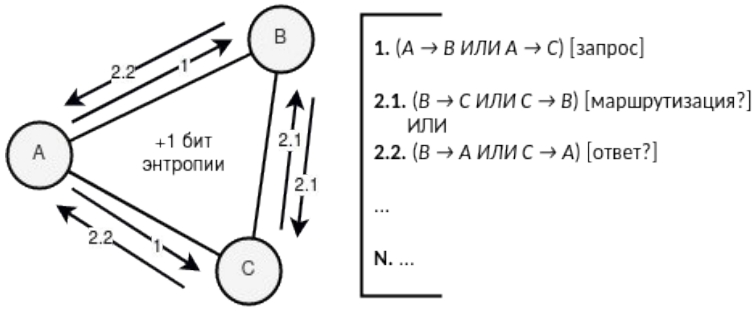

Рисунок 20. Зарождение неопределённости при вероятностном полиморфизме

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

1. Симуляция времени запроса. Иными словами, маршрутизация и ответ будут подстраиваться под примерное время генерации пакета в сети, способом установления задержки. Чем больше узлов в сети, тем меньше время задержки. Подобный метод следует использовать только в системах с большим количеством узлов, т.к. с малым количеством время ожидания маршрутизации или ответа будет достаточно долгим.

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

Теперь, если предположить, что существует сговор активного внутреннего наблюдателя и пассивного глобального наблюдателя, то вырисовывается картина неблагоприятная для получателя, т.к. она в конечном счёте будет представлять его деанонимизацию. И правда, если отправитель становится способным формировать собственный маршрут, а также следить за сценарием работы сети посредством знания всех полиморфных состояний своего пакета, то последний узел из списка маршрутизации станет

тем, кто выдаст детерминированно ответ на поставленный запрос, и как следствие, самостоятельно создаст изоморфную связь между сетевой и криптографической идентификациями путём выдачи состояния объекта.

Решением должно стать отнесение отправителя ко множеству внешних атакующих, сделать его пассивным анализатором, прослушивателем системы на моменте получения пакета принимающей стороной и последующим транспортированием объекта до инициирующей стороны. Дополнительное формирование собственных маршрутов на принимающих узлах может стать частичным или составным решением проблемы, как это изображено на *Рисунке 21*, и привести к полиморфизму вида [(*A* → *B ИЛИ A* → *C*) → (*B* → *C ИЛИ C* → *B*)] → [(*B* → *C ИЛИ C* → *B*) → (*B* → *A ИЛИ C* → *A*)], где [] представляет раздельную генерацию маршрутизации пакета. Следовательно, вероятностный полиморфизм станет определением совокупной возможности существования промежуточных субъектов $^{3}/_{4} = {}^{1}/_{4}$ (со стороны отправителя) + $^{1}/_{4}$ (со стороны получателя) + $^{1}/_{4}$ (со стороны обоих узлов) и их отсутствия $^{1}/_{4}$, Таким образом, инициатор связи в конечном счёте станет неспособным со 100% уверенностью определить, что последний узел отправляющий пакет, станет тем самым истинным получателем сообщения.

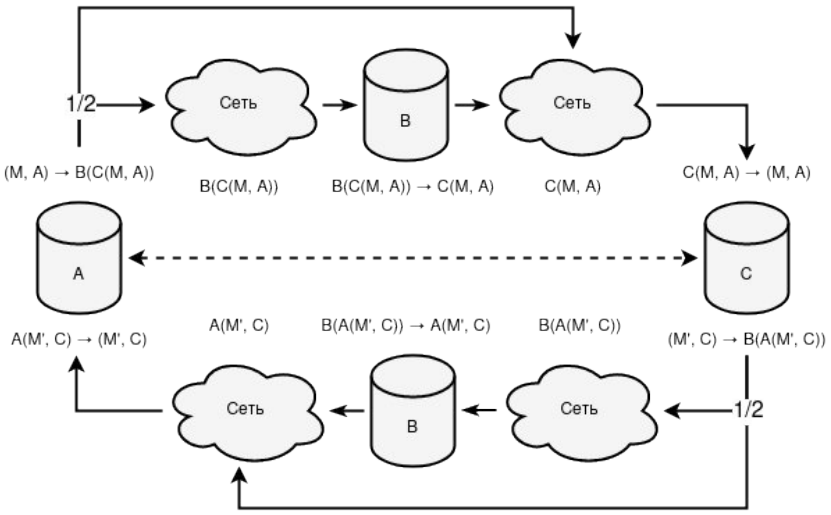

Рисунок 21. Обобщённая схема передачи информации в анонимной сети на базе увеличения энтропии

Но даже в вышеописанном случае остаётся связь при которой получатель должен будет первым формировать всю последующую маршрутизацию, а следовательно и первым, кто будет генерировать новый полиморфный пакет. И т.к. инициатор способен анализировать всю сеть, то выявить субъекта генерирующего пакет отличный от маршрутизирующего первоначально, на первый взгляд, не составит больших проблем. Но данная задача лежит в плоскости долгосрочного наблюдения за субъектами, а не краткосрочного. Проблематика деанонимизации такого случая усложняется алеаторными факторами (каждый промежуточный узел имеет вероятность генерировать псевдо-пакет, симуляция времени маршрутизации и ответа будет постоянно приводить к спаму, получатель способен самолично выставлять задержки отлика) порождающими и накапливающими энтропию, которая, как следствие, накладываясь на данную задачу, делает её анализ не таким примитивным и тривиальным — *Рисунок 22*.

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

Метаморфозы вероятностного полиморфизма	Расширение энтропии
1. (*A* → *B ИЛИ A* → *C*) [# *A* - инициатор] [# *B или C* - получатель]	1. [запрос(1)] → | 0 бит |
2. (*B* → *C ИЛИ C* → *B*) [# $T_{[0;N]}$] [# *B или C* - маршрутизатор] *ИЛИ* (*B* → *C ИЛИ C* → *B*) [# *B или C* - отправитель]	1. [маршрутизация(1)] = 2. [запрос(2)] → | 1 бит |
3. (*B* → *A ИЛИ C* → *A*) [# $T_{[0;N]}$] [# *B или C* - получатель]	3. [ответ(1)] → | 1 бит |

В такой концепции свойство задержки $T_{[0;N]}$ применяется для аккумулирования энтропии. Чем больше участников сети становится, тем бо́льший прирост энтропии способен обеспечиваться в интервале $T_{[0;N]}$. При отсутствии данного параметра вероятность нулевого прироста энтропии увеличивается прямо пропорционально уменьшению мощности спама[6]

---

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

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

где F: $N \cup \{0\} \to \{0, 1\} = \left\lceil \frac{x}{1+x} \right\rceil$ => $0 \to 0$; $x \neq 0 \to 1$,

G: $\{0, 1\} \to \{0, 1\} = x + 1 \pmod 2$ => $0 \to 1$; $1 \to 0$,

$L = Q(N)$,

N – множество всех узлов в сети,

Q – функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами,

Z – множество всех целых чисел,

P – период генерации пакета на базе выбранного узла.

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

	t_1	t_2	t_3	t_4	t_5	t_6
A	+	+	+	+	+	+

(активности) сети. Таким образом, максимальный диапазон задержки N должен устанавливаться не меньше среднего времени генерации нового пакета в системе.

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

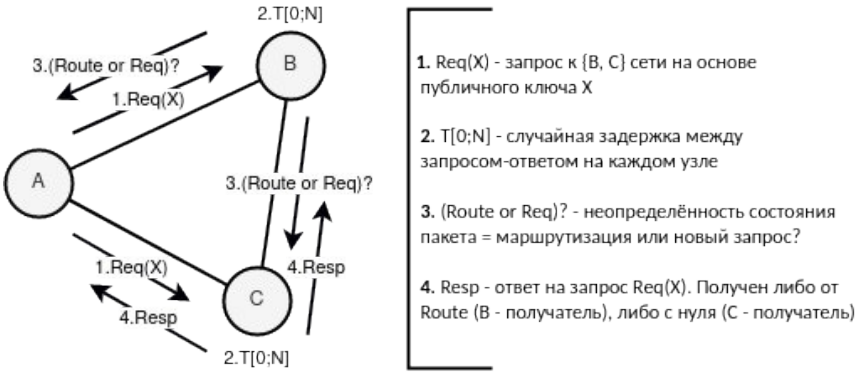

Рисунок 22. Неопределённость выявления получателя при атаке сопоставления связей между сетевой и криптографической идентификациями на инициирующей стороне

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

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

Отрицательными характеристиками сети на базе увеличения энтропии, в сравнении с сетью на базе очередей, являются необходимость в полиморфной маршрутизации (в том числе и при доверенных соединениях), а также необходимость в контроле накапливания

B	-	+	-	+	-	+
C	-	-	+	-	-	+
D	-	+	-	+	-	+
	$\|S_t\| = 1$	$\|S_t\| = 2$	$\|S_t\| = 2$	$\|S_t\| = 2$	$\|S_t\| = 1$	$\|S_t\| = 3$

энтропии. Данные случаи могут достаточно сильно усложнять систему и приводить к неправильным программным реализациям.

5.3. Модель на базе DC-сетей

Ещё одну из множества возможных моделей можно построить на базе существующих скрытых систем вида DC-сетей, с присущей им теоретически-доказуемой анонимностью. По умолчанию сети на базе «проблемы обедающих криптографов» не являются абстрактными, потому как привязаны к своей сетевой топологии типа «полносвязная» (как будет описано в подразделе «Анализ сетевых коммуникаций», типа связи «все-ко-всем»). В такой архитектуре исключается возможность вариативного расположения узлов по всему множеству сетевых коммуникаций. Допустим, в чистом виде DC-сети нельзя применять так, чтобы вычисление результата проходило только через одного участника, потому как таковой в последствии будет способен деанонимизировать всех остальных субъектов и переведёт анонимную сеть в этап второй стадии анонимности.

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

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

5.4. Анализ сетевых коммуникаций

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

представления связей «*один-к-одному*» и «*все-к-одному*» при помощи трёх субъектов. Поэтому минимальной структурой представления сетевых коммуникаций является связь «*все-ко-всем*» с тремя участниками сети.

В общем виде, существует всего три основных типа связей, как это представлено на *Рисунке 23*, в то время как все остальные соединения являются лишь их побочными гибридами.

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

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

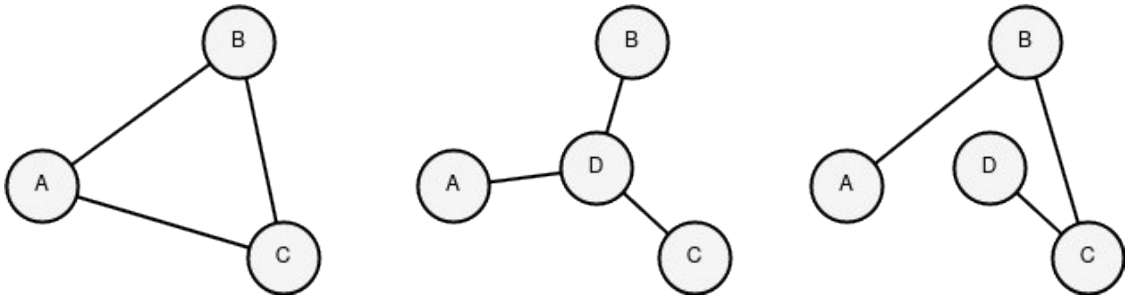

Рисунок 23. Связи: «*все-ко-всем*», «*все-к-одному*», «*один-к-одному*» (слева направо)

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,

инициализируется общий эквивалент представленный в формации соединений *«все-ко-всем»*.

Далее, если предположить, что существует четыре субъекта {*A, B, C, D*} со связью *«все-к-одному»*, где центральным узлом является точка *D*, то анализ безопасности абстрактной анонимной сети будет сводиться к осмотру действий от узла *D* ко всем остальным субъектам и от любого другого узла к субъекту *D*. В одном случае будет происходить прямая широковещательная связь, в другом же случае, будет происходить передача сообщения для последующей множественной репликации.

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 утверждено ранее, абстрактная сеть невосприимчива к такому виду деанонимизации. Следовательно, узел *D* становится словно фантомом, ретранслирующим субъектом не влияющим на безопасность и анонимность сети, базируемой на связи *«все-к-одному»*. Из этого также следует, что абстрактная система может применяться и в тайных каналах связи, где безопасность приложения выстраивается в заведомо подконтрольной, враждебной и централизованной инфраструктуре.

Теперь, если субъект *D* способен генерировать информацию, то создавая сеть и 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»* относительно каждого отдельного субъекта, коим и является узел *D*, а это, в свою очередь приводит к классическому (ранее заданному) определению абстрактной анонимной сети. Таким образом, связь «*все-к-одному*» внутри себя уже содержит логическую составляющую связи *«все-ко-всем»* через которую и доказывается её безопасность.

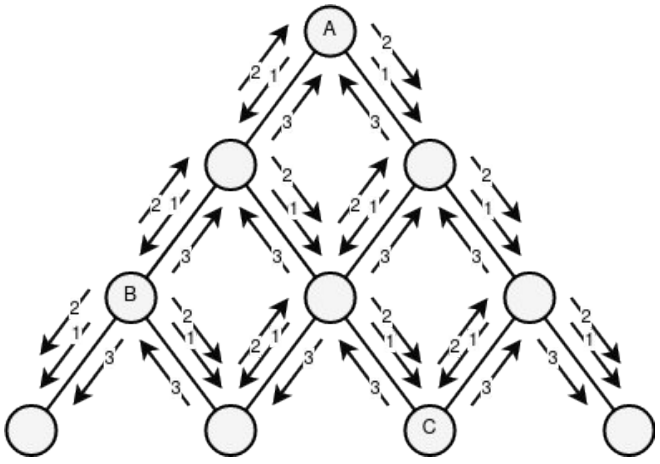

Рисунок 24. Маршрутизация пакета на базе абстрактной анонимной сети из 10 узлов, где *A* - отправитель, *B* - маршрутизатор, *C* - получатель

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

Далее, если предположить, что существует четыре субъекта {*A, B, C, D*} со связью *«один-к-одному»*, то базируясь на итеративности передачи информации в децентрализованных системах, можно декомпозировать любую модель в более замкнутую. Таким образом, сеть {*A, B, C, D*} фактически может расщепиться на две подсети {*A, B, C*} и {*B, C, D*}, мостом 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*», и как следствие, ко связи *«все-ко-всем»*.

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

6. Монолитный криптографический протокол

Ядром всех скрытых систем являются криптографические протоколы. Наиболее приоритетными протоколами, в конечном счёте, становятся простые, легкочитаемые и легкореализуемые. В массе своей, практические составляющие реального мира часто приводят к необходимости выбирать компромиссы между теоретической безопасностью и практической производительностью. В нашем же примере, будет представлен протокол направленный на поддержание конкретно теоретической безопасности, как главной цели, исключая какие бы то ни было компромиссы. Это может показаться слишком безрассудным, тем не менее, протокол останется практически реализуемым и даже применимым. Таковой, по концепции, будет схож с протоколом Bitmessage. Главной особенностью протокола станет его самодостаточность [48, с.80] и простота [23, с.58], а также возможность применения в тайных каналах и анонимных сетях (включая абстрактные системы).

6.1. Определение и программная реализация

Протокол определяется восьмью шагами, где три шага на стороне отправителя и пять шагов на стороне получателя. Для работы протокола необходимы алгоритмы КСГПСЧ (криптографически стойкого генератора псевдослучайных чисел), ЭЦП (электронной цифровой подписи), криптографической хеш-функции, установки / подтверждения работы, симметричного и асимметричного шифров.

Участники протокола:
A - отправитель,
B - получатель.
Шаги участника A:
1. K = G(N), R = G(N),
где G - функция-генератор случайных байт,
N - 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. $C_P = [\ E(\ PubK_B, K\ ), E(\ K, PubK_A\ ), E(\ K, R\ ), E(\ K, P\ ), H_P, E(\ K, S(\ PrivK_A, H_P\ )\ ), W(\ C, H_P\ )\ ],$

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

Шаги участника B:

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

где P_W - функция проверки работы.
Если ≠, то протокол прерывается.

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

где D - функция расшифрования.
Если ≠, то протокол прерывается.

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

Если ≠, то протокол прерывается.

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

где V - функция проверки подписи.
Если ≠, то протокол прерывается.

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

Если ≠, 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.

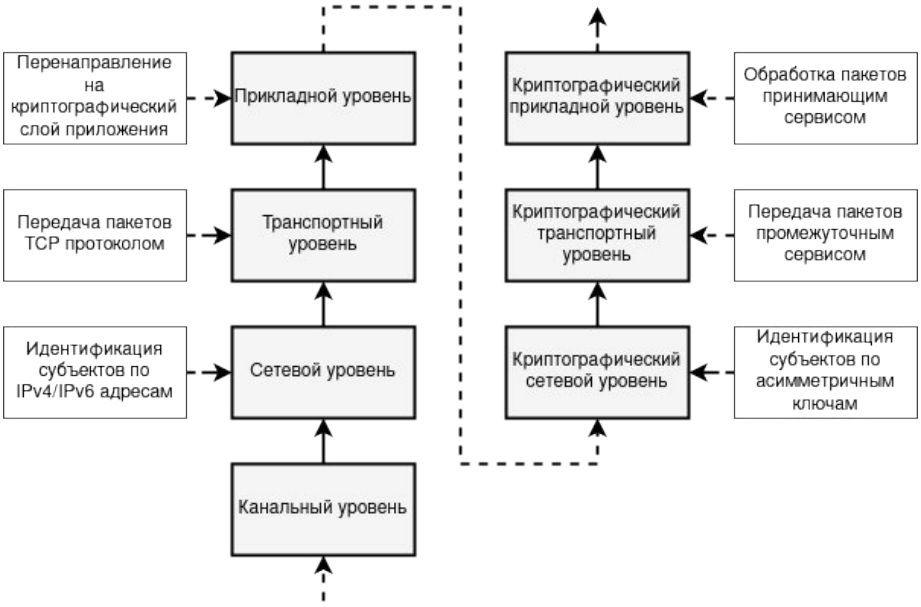

Рисунок 25. Расширение стека протоколов TCP/IP на базе криптографических абстракций

Также протокол способен игнорировать сетевую идентификацию субъектов информации, замещая её идентификацией криптографической. При таком подходе

аутентификация субъектов начинает становиться сингулярной функцией, относящейся лишь и только к асимметричной криптографии, и как следствие, прикладной уровень стека TCP/IP начинает симулятивно заменять криптографический слой по способу обнаружения отправителя и получателя, как это показано на *Рисунках 25, 26*. Из вышеописанного также справедливо следует, что для построения полноценной информационной системы необходимым является симулятивная замена транспортного и прикладного уровня последующими криптографическими абстракциями. Под транспортным уровнем может пониматься способ передачи сообщений из внешней (анонимной сети) во внутреннюю (локальную), под прикладным — взаимодействие со внутренними сервисами.

Сеанс связи в приведённом протоколе определяется самим пакетом, или иными словами один пакет становится равен одному сеансу за счёт генерации случайного сеансового ключа. Описанный подход приводит к ненадобности сохранения фактического сеанса связи, исключает внешние долговременные связи между субъектами посредством имманентности и абстрагирования объектов, что приводит к невозможности рассекречивания всей информации, даже при компрометации одного или нескольких сеансовых ключей.

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.

Пример программного кода [49][50] для шифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Encrypt(sender *PrivateKey, receiver *PublicKey, data []byte) *Package {
	var (
		pubsend		= PublicKeyToBytes(&sender.PublicKey)
		session		= GenerateBytes(N)
		randBytes	= GenerateBytes(N)
	)

	hash := HashSum(bytes.Join(
		[][]byte{
			randBytes,
			data,
			pubsend,
			PublicKeyToBytes(receiver),
		},
		[]byte{},
	))

	return &Package{
		Head: HeadPackage{
			Sender:		EncryptS(session, pubsend),
			Session:	EncryptA(receiver, session),
			RandBytes:	EncryptS(session, randBytes),
		},
		Body: BodyPackage{
			Data:	EncryptS(session, data),
```

```
                    Hash:   hash,
                    Sign:   EncryptS(session, Sign(sender, hash)),
                    Proof:  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.

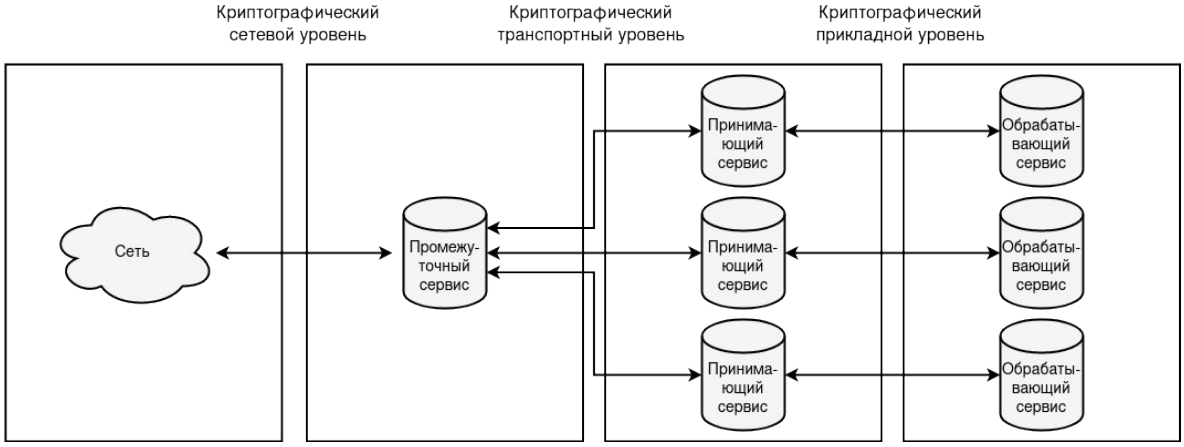

Рисунок 26. Расширенный стек протоколов на примере сервисов в анонимной сети

Использование одной и той же пары асимметричных ключей для шифрования и подписания не является уязвимостью, если применяются разные алгоритмы кодирования [23, с.257] или сама структура алгоритма представляет различные способы реализации. Так например, при алгоритме RSA для шифрования может использоваться алгоритм OAEP, а для подписания – PSS. В таком случае не возникает «подводных камней» связанных с возможным чередованием «шифрование-подписание». Тем не менее остаются риски связанные с компрометацией единственной пары ключей, при которой злоумышленник сможет не только расшифровывать все получаемые сообщения, но и подписывать отправляемые [48, с.99][48, с.291]. Но этот критерий также является и относительным плюсом, когда личность субъекта не раздваивается и, как следствие, данный факт не приводит к запутанным ситуациям чистого отправления и скомпрометированного получения (и наоборот).

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 может уходить продолжительное количество 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.

Недостатком протокола является отсутствие последовательности между несколькими пакетами. Иными словами невозможно определить нумерацию, что в некой степени переводит часть полноценного протокола на логику приложения, как например передача файлов. Это, в свою очередь, обосновывается упрощением протокола, где не требуются хранилище или база данных для хранения последовательности пакетов со стороны каждого входящего объекта. Также в некоторых приложениях последовательность сообщений не критична, как например в электронной почте или мессенджерах, где необходим лишь сам факт уже существующего дубликата (данный момент можно проверять хешем пакета).

Другим недостатком является постоянное применение функции подписания, которая считается наиболее ресурсозатрачиваемой, с практической точки зрения, операцией. При большом количестве поступаемых сообщений, возникнет и необходимость в большом количестве проверок подписания. При этом использование MAC, взамен ЭЦП, является недопустимым, потому как таковая имитовставка создаст буквально поточную связь между субъектами информации (создаст дополнительные связи между субъектами и генерируемым объектом), усложнит протокол и может привести теоретически к более чем одному возможному вектору нападения на протокол.

Для улучшения эффективности, допустим при передаче файлов, 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 хеш-значением 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.

Пример программного кода для расшифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Decrypt(receiver *PrivateKey, pack *Package) (*PublicKey, []byte) {
	// Check hash size.
	If len(pack.Body.Hash) != HashSize {
		return nil, nil
	}

	// Check proof of work.
	if !ProofIsValid(pack.Body.Hash, C, pack.Body.Proof) {
		return nil, nil
	}

	// Decrypt session key.
	session := DecryptA(receiver, pack.Head.Session)
	if session == nil {
		return nil, nil
	}

	// Decrypt public key.
	bpubsend := DecryptS(session, pack.Head.Sender)
	if bpubsend == nil {
		return nil, nil
	}
	pubsend := BytesToPublicKey(bpubsend)
	if pubsend == nil {
```

```
			return nil, nil
		}
		pubsize := PublicKeySize(pubsend)
		if pubsize  != KeySize {
			return nil, nil
		}

		// Decrypt rand bytes.
		randBytes := DecryptS(session, pack.Head.RandBytes)
		if randBytes == nil {
			return nil, nil
		}

		// Decrypt data.
		data := DecryptS(session, pack.Body.Data)
		if data == nil {
			return nil, nil
		}

		// Check hash.
		check := HashSum(bytes.Join(
			[][]byte{
				randBytes,
				data,
				PublicKeyToBytes(pubsend),
				PublicKeyToBytes(&receiver.PublicKey),
			},
			[]byte{},
		))
		if !bytes.Equal(pack.Body.Hash, check) {
			return nil, nil
		}

		// Decrypt signature.
		sign := DecryptS(session, pack.Body.Sign)
		if sign == nil {
			return nil, nil
		}

		// Check signature.
		if !Verify(pubsend, pack.Body.Hash, sign) {
			return nil, nil
		}

		return pubsend, data
	}
```

Протокол также способен обеспечивать полиморфизм информации методом 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, 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 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
}
```

Весь представленный программный код на языке Go представлен только как шаблон, показывающий способ шифрования и расшифрования непосредственно. Проблемой здесь является простота и примитивность анализа сетевого трафика по JSON-формату, что может привести к последующим блокировкам всех сетевых построений на основе данного код, а также игнорирование факта изменения размерности пакета, что может привести к деанонимизации субъектов информации (более подробно в подразделе «Противодействие обнаружению динамики размерности пакетов»). Необходимым решением предотвращения простоты анализа трафика должно служить вынесение сеансового ключа за пакет JSON-формата, последующее шифрование им пакета и конкатенация зашифрованного пакета с шифрованным сеансовым ключом. Если размер асимметричного ключа заведомо известен, то будет известен и размер зашифрованного сеансового ключа, что не приведёт к каким-либо проблемам расшифрования информации.

Другая проблема заключается в отсутствии каких бы то ни было видимых метаданных (хеш-значения, доказательства работы), которые бы помогли в борьбе со спамом, что в свою очередь является крайне важным критерием для большинства децентрализованных систем. Таким образом, отсутствие метаданных равносильно отсутствию отказоустойчивости, что отсылает на противоречие эквивалентности полностью анализируемого и неподверженного анализу пакетам. Одним из возможных решений данной проблемы может служить использование общепринятного и стандартизированного протокола типа SSL/TLS с целью сокрытия факта использования монолитного протокола.

6.2. Противодействие обнаружению динамики размерности пакетов

Теперь, если анализировать непосредственно сами пакеты, в моменты их перемещения по сети, то можно наблюдать точно заданную тенденцию при которой их размер будет

стремиться 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[7], 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 посредством 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 уже 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 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 целью, чтобы маршрутизатор мог дополнять пакет на некую величину размера M[8], приводящую к константному размеру K[9] [27, с.6].

---

[7]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.

[8]Переменная величина M применяется для замещения удалённых слоёв шифрования, сохраняя

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 абстрактной скрытой системы, 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.

Ещё одним и более корректным способом решения проблемы является использование случайной величины R[10], 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 и большего размера (чем истинный пакет) 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 «раскрыть» пакет, тем самым уменьшив его размер.

размер любой стадии полиморфного пакета на уровне константной величины K.

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

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

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

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

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

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

2. Если новый пакет меньше предыдущего, то субъектом данного объекта является маршрутизатор.

Ложно, т.к. ответ может быть меньше запроса.

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.

Для второго и четвёртого пунктов также действенно следующее правило — если истинный запрос/ответ по логике приложения всегда меньше ответа/запроса, то положение вероятностным образом меняется на противоположное при использовании переменных величин $\{V_1, V_2, ..., V_n\}$.

7. Заключение

Ключевым аспектом данной работы стал анализ развития сетевых коммуникаций, сетевых архитектур и, как следствие, сетевой анонимности. Было дано определение анонимности и стадий её становления, каждая из которых формировалась посредством двух составляющих – мощности доверия и мощности анонимности. Было выявлено шесть основных стадий анонимности и две противоречивые формы в лице первой^ и пятой^ стадий. Таковые стадии становятся лишь частными случаями общей теории, но не менее значимыми, т.к. первая^ стадия выявила второй вектор развития анонимных сетей, в то время как пятая^ стадия доказала своим существованием неэквивалентность принадлежности скрытых сетей последней градации анонимата. Также было выявлено противоречие, при котором стремление к уменьшению мощности доверия становилось второстепенным свойством, как только достигался этап формирования анонимной сети. Решением проблемы стало объединение пятой стадии анонимности со стадией скрытой сети. На основе базового развития анонимности и, в частности скрытых сетей, было выявлено существование абстрактных анонимных сетей, как нового класса, где способ распространения информации и первичная архитектура сети более не имели решающего значения. Из этого следовало, что таковые системы способны функционировать даже будучи расположенными в заведомо враждебных и прослушиваемых окружениях. Благодаря таковым свойствам, абстрактные анонимные сети способны применяться и в тайных каналах связи. Было представлено два вида абстрактных анонимных сетей: на базе очередей и на базе увеличения энтропии. Обе системы представляют теоретически доказуемую анонимность, но разными методами. Также в статье был представлен монолитный криптографический протокол, который может применяться для разного рода скрытых систем: клиент-безопасные приложения, тайные каналы связи, анонимные сети (в том числе и абстрактные). Были описаны основные преимущества и недостатки данного протокола, а также приведён пример программного кода. После монолитного криптографического протокола были перечислены основные методы сокрытия факта изменения размера информации по мере перехода от одного маршрутизирующего узла к другому.

Список литературы

1. Кан, Д. Взломщики кодов / Д. Кан. — М.: ЗАО Изд-во Центрполиграф, 2000. - 473 с.
2. Сингх, С. Тайная история шифров и их расшифровки / С. Сингх. — М.: АСТ: Астрель, 2009. - 447 с.
3. Граймс, Р. Апокалипсис криптографии / Р. Граймс. — М.: ДМК Пресс, 2020. - 290 с.
4. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.
5. Попова, А. Интернет как сетевая или иерархическая структура: концепция сети в постмодернистской философии и социальных науках конца XX-го и начала XXI-го вв. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/internet-kak-setevaya-ili-ierarhicheskaya-struktura-kontseptsiya-seti-v-postmodernistskoy-filosofii-i-sotsialnyh-naukah-kontsa-xx-go-i (дата обращения: 02.01.2022).
6. Бодрийяр, Ж. Символический обмен и смерть / Ж. Бодрийяр. — М.: РИПОЛ классик, 2021. – 512 с.
7. Шнайер, Б. Beyond Security Theater [Электронный ресурс]. — Режим доступа: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html (дата обращения: 16.03.2022).
8. Меньшиков, Я., Беляев, Д. Утрата анонимности в век развития цифровых технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/utrata-anonimnosti-v-vek-razvitiya-tsifrovyh-tehnologiy (дата обращения: 04.01.2022).
9. Молчанов, А. Парадокс анонимности в Интернете и проблемы ее правового регулирования [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/paradoks-anonimnosti-v-internete-i-problemy-ee-pravovogo-regulirovaniya (дата обращения: 12.07.2022).
10. Симаков, А. Анонимность в глобальных сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/anonimnost-v-globalnyh-setyah (дата обращения: 04.01.2022).
11. Рабинович, Е., Шестаков, А. Способ управления трафиком в BitTorrent-сетях с помощью протокола DHT [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnaya-reaktsiya-na-deystviya-edvarda-snoudena (дата обращения: 26.09.2022).
12. Зденек, Ш. Международная реакция на действия Эдварда Сноудена [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnaya-reaktsiya-na-deystviya-edvarda-snoudena (дата обращения: 26.09.2022).
13. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. - СПб.: Питер, 2003. - 368 с.
14. 5-5-3-5: проще штрафы платить, чем ИБ внедрять [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/dsec/blog/677204/?ysclid=l8iii2g114542316743 (дата обращения: 26.09.2022).
15. Спраул, М. Антимонопольная практика и цены [Электронный ресурс]. — Режим доступа: https://prompolit.ru/files/560276/sproul.pdf (дата обращения: 26.09.2022).
16. Иванов, А. Мифы о легальной монополии, или сказ о том, почему в России не развиваются инновации при упорной охране интеллектуальной собственности [Электронный ресурс]. — Режим доступа: https://www.hse.ru/data/2020/03/16/1565183163/086-102_%D0%B8%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2.pdf?ysclid=l8ihr02tc6145956359 (дата обращения: 26.09.2022).

17. Смыгин, К. Тайные сговоры, повышение цен, рост безработицы и другие риски, которые таят в себе монополии. Ключевые идеи из бестселлера «Миф о капитализме» [Электронный ресурс]. — Режим доступа: https://rb.ru/opinion/mif-o-kapitalizme/?ysclid=l8ii06vu6s628640881 (дата обращения: 26.09.2022).
18. Анохин, Ю., Янгаева, М. К вопросу о MITM-атаке как способе совершения преступлений в сфере компьютерной информации [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-mitm-atake-kak-sposobe-sovershеniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 04.01.2022).
19. Иванович, Я. Может ли быть "монополия без монополиста"? [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mozhet-li-byt-monopoliya-bez-monopolista (дата обращения: 26.09.2022).
20. Молоков, В. К вопросу о безопасном шифровании в интернет-мессенджерах [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-bezopasnom-shifrovanii-v-internet-messendzherah (дата обращения: 04.01.2022).
21. Вишневская, Ю, Коваленко, М. Анализ способов и методов незаконного распространения личных данных пользователей мессенджеров, социальных сетей и поисковых систем [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/analiz-sposobov-i-metodov-nezakonnogo-rasprostraneniya-lichnyh-dannyh-polzovateley-messendzherov-sotsialnyh-setey-i-poiskovyh-sistem (дата обращения: 30.12.2021).
22. Diffie, W., Hellman, M. New Directions in Cryptography [Электронный ресурс]. — Режим доступа: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 19.12.2020).
23. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. - М.: Издательский дом «Вильямс, 2005. - 420 с.
24. Соснин, М. Реализация оптимальной архитектуры и Обеспечение безопасного функционирования сети ЭВМ [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/realizatsiya-optimalnoy-arhitektury-i-obespechenie-bezopasnogo-funktsionirovaniya-seti-evm (дата обращения: 26.09.2022).
25. Михайленко, Н., Мурадян, С., Вихляев, А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/aktualnye-voprosy-monitoringa-i-protivodeystviya-kiberugrozam-v-odnorangovyh-setyah (дата обращения: 26.09.2022).
26. Садаков, Д., Сараджишвили, С. Рекомендательный протокол децентрализованной файлообменной сети [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/rekomendatelnyy-protokol-detsentralizovannoy-fayloobmennoy-seti (дата обращения: 29.03.2022).
27. Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Электронный ресурс]. — Режим доступа: https://www.lix.polytechnique.fr/~tomc/P2P/Papers/Theory/MIXes.pdf (дата обращения: 16.08.2022).
28. Ершов, Н., Рязанова, Н. Проблемы сокрытия трафика в анонимной сети и факторы, влияющие на анонимность [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/problemy-sokrytiya-trafika-v-anonimnoy-seti-i-faktory-vliyayuschie-na-anonimnost (дата обращения: 02.01.2022).
29. NETSUKUKU RFC документация [Электронный ресурс]. — Режим доступа: http://netsukuku.freaknet.org/sourcedocs/main_doc/ntk_rfc/ (дата обращения: 31.12.2021).

30. Danezis, G., Diaz, C., Syverson, P. Systems for Anonymous Communication [Электронный ресурс]. — Режим доступа: https://www.esat.kuleuven.be/cosic/publications/article-1335.pdf (дата обращения: 27.09.2022).
31. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер. — СпБ.: ООО «Альфа-книга», 2018. - 1040 с.
32. Шелухин, О., Канаев, С. Стеганография. Алгоритмы и программная реализация / О. Шелухин, С. Канаев. — М.: Горячая линия - Телеком, 2018. - 592 с.
33. Карпов, Д., Ибрагимова, З. Способы и средства обеспечения анонимности в глобальной сети Интернет [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/sposoby-i-sredstva-obespecheniya-anonimnosti-v-globalnoy-seti-internet (дата обращения: 15.07.2022).
34. Рябко, Е. Калейдоскоп vpn технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kaleydoskop-vpn-tehnologiy (дата обращения: 02.01.2022).
35. 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).
36. Warren, J. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System [Электронный ресурс]. — Режим доступа: https://bitmessage.org/bitmessage.pdf (дата обращения: 31.12.2021).
37. Perry, M. Securing the Tor Network [Электронный ресурс]. — Режим доступа: https://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-perry-WP.pdf (дата обращения: 03.01.2022).
38. Astolfi, F., Kroese, J., Oorschot, J. I2P - Invisible Internet Project [Электронный ресурс]. — Режим доступа: https://staas.home.xs4all.nl/t/swtr/documents/wt2015_i2p.pdf (дата обращения: 03.01.2022).
39. Danezis, G., Dingledine, R., Mathewson, N. Mixminion: Design of a Type III Anonymous Remailer Protocol [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20170312061708/https://gnunet.org/sites/default/files/minion-design.pdf (дата обращения: 03.01.2022).
40. Рябко, Б., Фионов, А. Криптография в информационном мире / Б. Рябко, А. Фионов. - М.: Горячая линия - Телеком, 2019. - 300 с.
41. Chaum, D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability [Электронный ресурс]. — Режим доступа: https://www.cs.cornell.edu/people/egs/herbivore/dcnets.html (дата обращения: 24.07.2022).
42. Goel, S., Robson, M., Polte, M., Gun Sirer, E. Dissent in Numbers: Making Strong Anonymity Scale [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/osdi12.pdf (дата обращения: 24.07.2022).
43. Corrigan-Gibbs, H., Wolinsky, D., Ford, B. Proactively Accountable Anonymous Messaging in Verdict [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/verdict.pdf (дата обращения: 24.07.2022).
44. Alonso, K., KOE. Zero to Monero: First Edition A technical guide to a private digital currency; for beginners, amateurs, and experts [Электронный ресурс]. — Режим доступа: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf (дата обращения: 28.12.2021).
45. Duffield, E., Diaz, D. Dash: Privacy-Centric Crypto-Currency [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20150514080026/https://www.dashpay.io/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf (дата обращения: 28.12.2021).

46. Popescu, B., Crispo, B., Tanenbaum, A. Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System [Электронный ресурс]. — Режим доступа: http://turtle-p2p.sourceforge.net/turtleinitial.pdf (дата обращения: 29.12.2021).
47. Шеннон, К. Теория связи в секретных системах [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20141222030352/http://pv.bstu.ru/crypto/shannon.pdf (дата обращения: 02.01.2022).
48. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. - М.: Издательский дом «Вильямс, 2005. - 420 с.
49. Донован, А., Керниган, Б. Язык программирования Go / А.А. Донован, Б.У. Керниган. — М.: ООО «И.Д. Вильямс», 2018. - 432 с.
50. Программная реализация протокола go-peer [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer (дата обращения: 20.03.2022).