Hidden Lake Service — ядро скрытой сети с теоретически доказуемой анонимностью

Коваленко Геннадий Александрович

Аннотация. Весь нижеизложенный материал является следствием основной статьи «Теория строения скрытых систем» [1]. Основные источники по тем или иным составляющим можно найти также найти в данной работе. Программная реализация ядра HLS представлена в библиотеке «go-peer» [2]. Основная статья и программный код находятся полностью в открытом доступе.

Ключевые слова. анонимность; сети; децентрализация; теоретическая доказуемость; проблема обедающих криптографов;

1. Введение

Анонимность всегда трактуется по разному. Некоторые люди под анонимностью понимают сокрытие идентификаторов пользователей, то есть использование псевдонимов. Другие люди под анонимностью представляют сокрытие (или запутывание) связей между отправителем и получателем. Ещё одни под анонимность понимают неопределённость факта отправления информации или её получения, то есть отсутствие возможности узнать отправляет ли какой-то пользователь информацию или же нет.

Данные определения также усугубляются тем фактом, что существует множество всеразличных атак и сама анонимность может быть различной по уровню анонимизации (может принадлежать разным моделям угроз). Как пример, факт отправления и получения сводится к более сложной моделе угроз, чем факт связывания отправителя и получателя между собой. Например, анонимная сеть может допускать разглашение истинности отправления информации и её получения, но не разглашать связь "отправление-получение". Иными словами, если существует множество отправителей и множество получателей, то задача сводится к тому, что сложно связать одного отправителя с одним получателем из двух данных множеств.

Скрытые сети с теоретически доказуемой анонимностью сводятся к наивысшей модели угроз, где становится невозможным (для пассивных внешних и внутренних атакующих) обнаружить сам факт отправления и факт получения информации. Иными словами, такие сети скрывают не только связь между субъектами, но и их роли (отправитель, получатель или просто держатель сети).

Сети с теоретически доказуемой анонимностью не являются новшеством. Как минимум, существуют DC-сети (проблема обедающих криптографов), такие как Herbivore и Dissent. Это говорит о том, что, в последующем, разбираемая сеть Hidden Lake Service (HLS) не будет являться какой-то уникальной системой. Она просто навсего будет говорить (своим существованием) об ещё одой возможной реализации скрытых сетей с теоретически доказумой анонимностью, не более.

2. Виды анонимности и векторы нападения

Чтобы понять сам смысл теоретически доказуемой анонимности и что под ней понимается, необходимо рассмотреть возможные атаки и нападения, совершаемые на анонимные сети, но перед этим лучше будет разобрать то, какие виды и возможные реализации анонимных сетей вообще существуют и к какой модели угроз они так или иначе принадлежат.

1. Анонимность связи между отправителем и получателем. Такие сети обладают самой слабой моделью угроз, потому как разглашают всем (или гипотетически всем) кто является отправителем и кто является получателем. Под анонимностью понимается лишь факт несвязанности между каким-то отправителем и каким-то получателем. Примером таковых сетей являются Tor, I2P, Mixminion. (Критерий несвязываемости)

2. Анонимность отправителя или получателя. Данная сеть имеет усреднённую модель угроз, в том плане, что она скрывает только факт отправления или только факт получения информации одним из субъектов (либо отправителем, либо получателем). (Критерий ненаблюдаемости)

Примером таковых сетей может являться сеть, где отправитель транспортирует полностью зашифрованное сообщение всем участникам сети, расшифровать которое может только тот, у кого есть приватный ключ ориентированный на данное сообщение (если здесь конечно используется асимметричная криптография). Теоретически все могут узнать отправителя информации, но узнать получателя и есть ли он вообще крайне проблематично, потому как в теории получателем может оказаться каждый, т.к. каждый получает эти сообщения.

Другим примером может являться сеть, где по определённому периоду T генерируется информация всеми участниками сети и отправляется одному серверу посредством нескольких маршрутизаторов несвязанных между собой общими целями и интересами (то есть не находятся в сговоре). Получатель-сервер расшифровывает всю информацию и (как пример) публикует её в открытом виде. Получатель всем известен - сервер, в то время как отправители скрыты.

3. Анонимность отправителя и получателя. Представляет выражение сильной модели угроз, потому как не даёт никакой информации о факте отправления и факте получения информации. Иными словами, предположим, что получателю всегда необходимо отвечать отправителю, иными словами создаётся модель типа "запрос-ответ". В такой системе становится невозможным применить "анонимность отправителя или получателя", т.к. отправитель рано или поздно станет получателем, а получатель - отправителем, а потому и модель угроз на базе второго типа начнёт регрессировать и станет моделью на базе первого типа - "анонимность связи между отправителем и получателем". (Критерий ненаблюдаемости)

Сами модели угроз могут быть описаны со стороны ряда атакующих. Так можно выделить четыре вида основных нападающих, которые могут быть описаны в виде представленной ниже таблицы.

	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

К внешним атакам следует относить нападения, которые фиксируют транспортирование информации от нескольких точкек сети при помощи анализа трафика, не находясь при этом в самой сети. Ко внутренним атакам следует относить нападения совершаемые посредством "вживления" в саму сеть и анализа её составляющей.

К пассивным атака относятся нападения совершаемые исключительно анализом принимаемых данных. К активным атакам относятся нападения совершаемые инициализацией какого-либо действия.

Примером внешней пассивной атаки (B) является анализ трафика сети от точки **a** до точки **b**. Примером внешней активной атаки (D) является блокирование определённых узлов в сети на уровне провайдеров или на локальном уровне. Примером внутренней пассивной атаки (A) является анализ принимаемого трафика от участников сети. Примером внутренней активной атаки (C) является отправление информации какой-либо точке с последующим анализом принятой информации в качестве ответа.

Стоит также заметить, что активные атаки являются надмножеством пассивных, иными словами множество A принадлежит C, множество B принадлежит D. Также множества {B, D} можно условно разделить на два подмножества {B1, D1} и {B2, D2}. Примем, что множество {B2, D2} есть множество атак со стороны внешнего глобального наблюдателя, а множество {B1, D1} без него соответственно. Глобальный наблюдатель - это частный случай внешнего наблюдателя, которому подвластна вся сеть в плане анализа её трафика. Таким образом, множество {B, D} = {B1 или B2, D1 или D2}. Объединение внешних и внутренних атакующих будем называть сговором.

Из данных определений уже можно выразить теоретически доказуемую анонимность.

Скрытая сеть с теоретически доказуемой анонимностью должна удовлетворять свойству замкнутости (быть невосприимчева к атакам глобального наблюдателя), в которой становится невозможным определение факта отправления и факта получения информации пассивными атакующими. 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.

При этом в определении теоретички доказуемой анонимности не лежит вектор активных нападений, потому как таковой может отличаться в зависимости от самой реализации сети. Поэтому теоретически доказуемая анонимность есть минимальный порог при котором сеть может доказанно противостоять пассивным нападениям в любой их форме.

3. DC-сети

Первой теоретически доказуемой анонимной сетью (как ядро) становится задача обедающих криптографов. Выглядит она так (не буду пересказывать о том, как криптографы обедают и о том, что существует некий АНБ, раскажу вкратце): существует три участника сети {A, B, C}. Один участник хочет послать 1 бит информации по сети (либо 1, либо 0 соответственно), но таким образом, чтобы другие субъекты не узнали кто отправил данную

информацию. Предполагается, что таковые участники соединены между собой, тем самым имеют безопасный канал связи, а также имеют расписание по которому в каждый момент времени T генерируется новый бит.

Предположим, что участник A хочет отправить информацию по сети так, чтобы {B, C} эту информацию получили, но не смогли узнать, кто действительно является отправителем. Иными словами, для B это может быть {A, C}, а для C это {A, B} с вероятностью 50/50. Все участники начинают согласовывать общий бит со своими соседями (в момент времени T, конечно же). Предположим, что участники {A, B} согласовали бит = 1, {B, C} = 1, {C, A} = 0.

Далее каждый участник сети XOR'ит (операция исключающее ИЛИ) биты со всех своих соединений: A = 1 xor 0 = 1; B = 1 xor 1 = 0; C = 0 xor 1 = 1. Данные результаты обмениваются по всей сети и XOR'ятся каждым её участником: 0 xor 1 xor 1 = 0. Это говорит о том, что участник A передал бит информации = 0. Чтобы субъект A мог передать бит = 1, ему необходимо добавить операцию НЕ в своём вычислении, то есть A = НЕ(1 xor 0) = 0. В итоге, все вычисления прийдут к такому результату: 0 xor 0 xor 1 = 1. Таким образом, становится возможным передать 1 бит информации полностью анонимно (конечно же со стороны определения теоретически доказуемой анонимности).

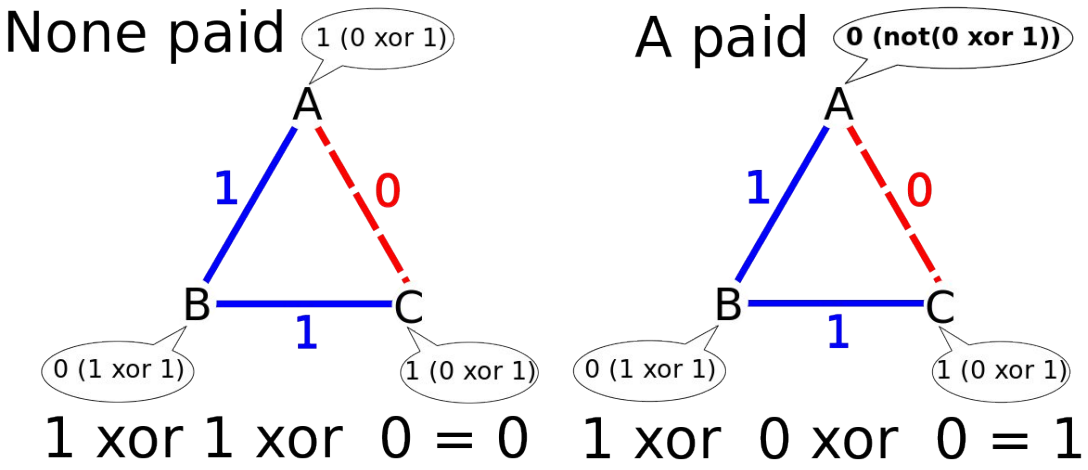

Рисунок 1. Сеть на базе задачи обедающих криптографов при трёх участниках {A, B, C}

Предположим, что один из участников, либо B, либо C захочет деанонимизировать либо {A, C}, либо {B, C} соответственно (то есть узнать, кто является отправителем информации). Тогда ему потребуется узнать согласованный секрет со стороны другой линии связи, что является сложной задачей (если конечно не был произведён сговор нескольких участников). Таким образом, атака со стороны внутреннего пассивного наблюдателя становится безрезультатной. Со стороны внешнего глобального наблюдателя такая же ситуация, потому как он видит лишь переадресации зашифрованных битов (потому как используется безопасный канал связи) в один момент времени T всеми участниками сети.

На этом примере также хорошо можно проиллюстрировать уязвимость к активным нападениям. Предположим, что данная сеть адаптируема под "запрос-ответ", иными словами любое действие инициатора (отправителя) будет порождать другое действие сервиса связи (получателя). Так предположим, что существует сговор активных внешних и внутренних атакующих. Внешний способен блокировать узлы в сети, а внутренний способен создавать

запросы к определённым узлам. На каждый запрос должен быть получен ответ. Предположим, что существует три участника {A, B, C}, где A - атакующий, задачей которого является деанонимизация другого субъекта {B, C}. Предположим, что у каждого участника существуют свои псевдонимы, благодаря которым они обмениваются информацией и благодаря такому свойству (отрыва от сетевой идентификации) становятся анонимными. Суть атаки - связать псевдоним с сетевым адресом.

Атака крайне проста (условно конечно же). Атакующий A генерирует запрос на участника B. Внешний наблюдатель блокирует один адрес, одного участника {B, C} соответственно. Если атакующий A получает ответ, тогда незаблокированный адрес является адресом участника B, иначе C (если ответ не был получен). Таким образом, активные нападения являются куда более серьёзным способом атак, но и их применимость может сводиться к разным условиям (в зависимости от архитектуры сети).

4. HLS

Теоретически доказуемая анонимная сеть HLS (как ядро) основана на базе очередей. В некоторой степени имеются схожие моменты с DC-сетями, тем не менее алгоритм приниципально отличается, как минимум из-за того, что таковой находится на более прикладном уровне со стороны криптографических протоколов и строит не широковещательную связь между субъектами. Иными словами HLS априори содержит в себе имплементацию E2E (сквозного) шифрования.

В отличие от DC-сетей, которые ограничивают как внутренних пользователей между собой (допустим отправитель и получатель не знают точные сетевые адреса друг друга), так и внешних (которые не участвуют в коммуникации), HLS ограничивает только внешних участников. Иными словами, предполагается, что участники априори знают друг друга, априори идентифицируют друг друга, а следовательно для них нет анонимности вообще. Поэтому такой вид сети теоретически более узконаправлен, чем DC-сети. Как минимум уже нельзя применять HLS для создания ботнет, чтобы скрывать адрес сервера или для создания сайтов с нехорошими товарами. Тем не менее, HLS будет полезен именно группе участников, которые переживают на счёт того, что их коммуникации будут увидены и проанализированы другими субъектами.

Такое свойство никак не противоречит теоретически доказуемой анонимности, потому как внутренние атакующие (в данном случае какие-либо ещё узлы сети кроме отправителя и получателя), а также внешние атакующие (анализирующие трафик сети) будут также неспособны узнавать о факте отправления, либо получения информации.

Вкратце суть HLS сводится к следующему: предположим, что существует три участника {A, B, C}. Каждый из них соединён друг к другу (что в сравнении с DC-сетями не является обязательным критерием, но данный случай я привёл исключительно для упрощения) (P.S. имеются реализации которые позволяют в DC-сетях не соединяться друг к другу, но данные способы скорее являются хаками, нежели вариативностью). Каждый субъект устанавливает время генерации информации = T. У каждого участника имеется своё внутренее хранилище по типу FIFO (первый пришёл - первый ушёл), можно сказать имеется структура "очередь".

Предположим, что участник A хочет отправить некую информацию одному из участников {B, C}, так, чтобы другой участник (или внешний наблюдатель()не знал что существует какой-либо факт отправления. Каждый участник в определённый период T генерирует сообщение. Такое сообщение может быть либо ложным (не имеющее никакого фактического содержания и никому по факту не отправляется, заполняясь случайными

битами), либо истинным (запрос или ответ). Отправить раньше или позже положенного времени T никакой участник не может. Если скопилось несколько запросов одному и тому же участнику, тогда он их ложит в свою очередь сообщений и после периода T достаёт из очереди и отсылает в сеть. Таким образом, сама структура HLS есть множество последовательно выстроенных очередей.

Таким образом, внешний глобальный наблюдатель будет видеть лишь картину, при которой каждый участник в определённо заданный период времени T отправляет некое сообщение всем остальным узлам сети, что не даёт никакой информации о факте отправления, либо получения. Внутренние пассивные участники также неспособны узнать коммуниицирует ли один из участников в данный период времени с каким-либо другим, т.к. предполагается, что шифрованная информация не выдаёт никаких данных об отправителе и получателе непосредственно.

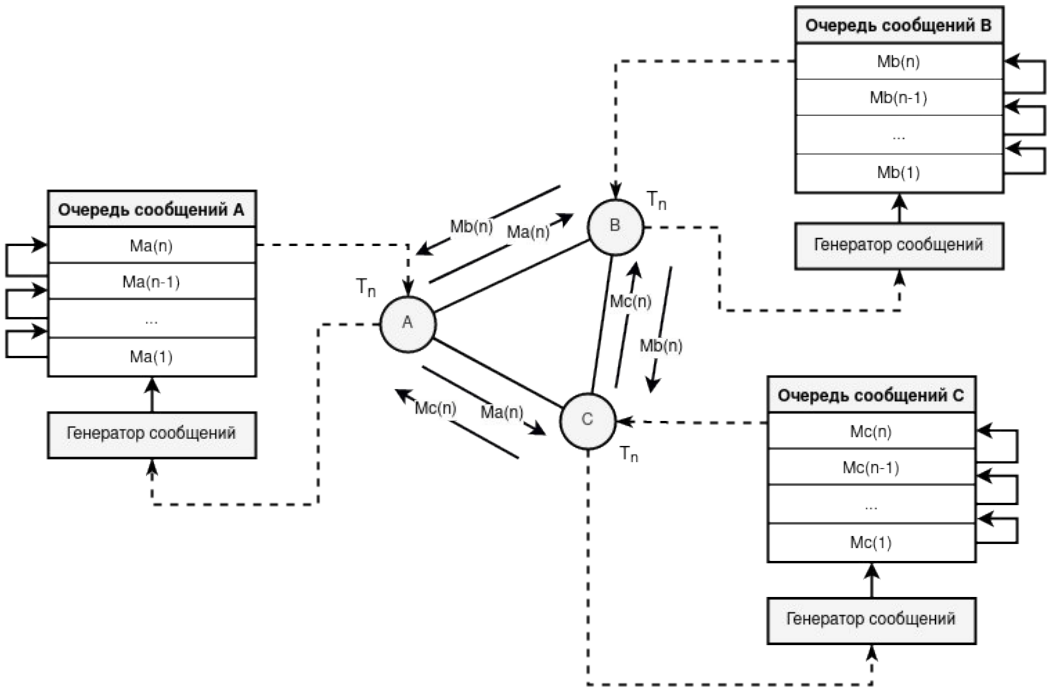

Рисунок 2. Сеть на базе очередей при трёх участниках {A, B, C}

Сеть HLS является по своей концепции F2F-сетью (friend-to-friend), потому как иначе (сли бы отсутствовала опция F2F), расширяясь она бы стала 1) тратить много ресурсов на попытки расшифрования информации, а следовательно если будет неограниченное количество участников вступать в сеть, то она просто ляжет; 2) если кто-то извне захочет за-DDoS-ить какого-либо участника, то он это легко сделает, просто перезагрузив очередь. Таким образом, HLS - это децентрализованная сеть доверенных соединений, в которой известны участники сети, но неизвестны случаи отправления и получения информации.

5. Заключение

Как было сказано в начале, сама сеть не является каким-то новшеством в плане теоретически доказуемой анонимности сетей, потому как таковые уже существовали и были вполне конкретно обозначены. Тем не менее, HLS - это теоретически доказуемая анонимность с новым типом реализации (на базе очередей), а потому вполне способна представлять некий самодостаточный интерес.

Список литературы

1. Коваленко, Г. Теория строения скрытых систем [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer/blob/master/hidden_systems.pdf (дата обращения: 01.11.2022).
2. Библиотека «go-peer» [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer (дата обращения: 01.11.2022).