НОРМАЛИЗАЦИЯ ТРАФИКА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО СКРЫТЫМ КАНАЛАМ

Епишкина А. В.[1], Когос К. Г.[2]

DOI: 10.21681/2311-3456-2024-5-4-17

Возможность построения скрытых каналов в информационной системе влечет за собой потенциальную утечку защищаемой информации. Существует множество методов противодействия скрытым каналам, однако не все они применимы на практике. Целью исследования является разработка методов противодействия утечке информации по скрытым каналам по памяти и по времени путем нормализации трафика.

В работе исследованы скрытые каналы по памяти и по времени, предложены алгоритмы полной и частичной нормализации трафика для противодействия указанных скрытым каналам. С использованием методов теории информации, теории вероятности, дифференциального и интегрального исчисления и данных о распределении длин межпакетных интервалов пакетов сетевого трафика выведены формулы для оценки эффективной пропускной способности канала связи в условиях противодействия скрытым каналам и остаточной пропускной способности скрытого канала.

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти, оценки пропускной способности которого показывают нецелесообразность применения частичной нормализации скрытого канала по времени и указывают на необходимость его полной нормализации.

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. В работе предложен способ противодействия, при котором скрытый канал по времени полностью уничтожается.

Рассчитаны количественные значения эффективной пропускной способности канала связи и остаточной пропускной способности скрытого канала при использовании протоколов IPv4 и IPv6, которые могут быть полезны при применении методов нормализации трафика на практике.

Ключевые слова: *информационная безопасность, утечка информации, метод противодействия, сетевой скрытый канал, скрытый канал по памяти, скрытый канал по времени, нормализация трафика, частичная нормализация, пропускная способность.*

Введение

В современном мире бесспорно актуальной является задача обеспечения информационной безопасности, от качества решения которой во многом зависит функционирование государственных и коммерческих организаций.

В настоящее время и на прогнозируемую перспективу сохранится тенденция широкого использования сетей пакетной передачи данных. Применение этих технологий привносит, а повсеместное внедрение делает весьма значимой угрозу негласного использования особенностей протокола IP для скрытой передачи информации ограниченного доступа по каналам связи, выходящим за пределы объектов информатизации, на которых она обрабатывается.

Необходимость создания и постоянного совершенствования способов противодействия утечке информации по так называемым скрытым каналам обусловлена и тем, что такие каналы могут быть построены в условиях применения традиционных способов сетевой защиты, заключающихся в межсетевом экранировании, туннелировании трафика и др. Исследования показывают, что данная угроза сохраняется даже при передаче информации в зашифрованном виде, более того, существуют так называемые необнаруживаемые скрытые каналы [1].

Впервые термин «скрытый канал» был введен в 1973 году Лэмпсоном (Lampson), который под скрытым каналом понимал канал связи, который не разрабатывался и не предполагался для передачи информации.

Скрытые каналы по механизму передачи информации подразделяют на:

- скрытые каналы по памяти [2–5];
- скрытые каналы по времени [6–10];
- статистические скрытые каналы [11].

Скрытые каналы по памяти основаны на наличии памяти, в которую передающий субъект записывает

1 Епишкина Анна Васильевна, кандидат технических наук, доцент, доцент кафедры криптологии и кибербезопасности НИЯУ МИФИ; доцент Инженерной академии РУДН, Москва, Россия. E-mail: avepishkina@mephi.ru

2 Когос Константин Григорьевич, кандидат технических наук, доцент, доцент кафедры криптологии и кибербезопасности НИЯУ МИФИ. Москва, Россия. E-mail: kgkogos@mephi.ru

информацию, а принимающий считывает ее. Скрытность каналов по памяти определяется тем, что сторонний наблюдатель не знает того участка памяти, где записана скрываемая информация, а поскольку способ использования памяти зачастую не учитывается разработчиками систем защиты, скрытые каналы указанного типа могут не выявляться используемыми средствами защиты.

Скрытый канал является каналом по памяти при выполнении следующих условий:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель имеет возможность изменить этот элемент разделяемого ресурса;
- получатель должен иметь возможность распознать такое изменение;
- должен существовать механизм синхронизации для отправителя и получателя для упорядочивания отправляемых данных;
- если не выбран специальный метод кодирования во избежание последовательности одинаковых символов, отправитель и получатель должны иметь возможность предварительно договориться о временном интервале, в течение которого получатель будет наблюдать за изменениями в канале.

Скрытые каналы по памяти подразделяют на следующие виды:

- скрытые каналы, основанные на сокрытии информации в структурированных данных (встраивание данных в информационные объекты с формально описанной структурой и формально описанными правилами обработки);
- скрытые каналы, основанные на сокрытии информации в неструктурированных данных (встраивание данных в информационные объекты в информационные объекты без учета формально описанной структуры).

Скрытые каналы по времени предполагают, что передающий информацию субъект моделирует с помощью передаваемой информации некий изменяющийся во времени процесс, а субъект, принимающий информацию, может демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени.

Скрытый канал является каналом по времени при выполнении следующих условий:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель и получатель должны иметь возможность синхронизировать свои действия;
- отправитель должен иметь возможность изменять время ответного сигнала получателя для выявления изменения в данном элементе разделяемого ресурса;
- должен быть механизм инициирования процесса передачи данных по скрытому каналу и упорядочивания отправляемых данных.

Скрытые статистические каналы используют для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытность таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не знающий структуру скрытого канала.

Скрытые каналы также можно разделить на каналы с шумом и каналы без шума [12]. Скрытые каналы с шумом — каналы, в которых вероятность верного распознавания переданных символов отлична от единицы. В частности, скрытый канал с шумом — канал, в котором наблюдаются как разрешенные, так и запрещенные политикой безопасности информационные потоки. В скрытом канале без шума общий ресурс используется исключительно скрытыми сторонами. Наличие шума важно учитывать при оценке пропускной способности скрытого канала. В частности, введение шума в скрытые каналы может применяться для ограничения пропускной способности скрытого канала.

По пропускной способности скрытые каналы подразделяют на следующие типы:

- каналы с низкой пропускной способностью (пропускной способности достаточно для передачи ценных информационных объектов минимального объема или команд за промежуток времени, на протяжении которого данная передача является актуальной);
- каналы с высокой пропускной способностью (пропускной способности достаточно для передачи информационных объектов среднего и большого размера за промежуток времени, на протяжении которого данные информационные объекты являются ценными).

Угрозы безопасности, которые могут быть реализованы с помощью скрытых каналов, включают в себя:

- внедрение вредоносных программ и данных;
- передачу злоумышленником команд агентам для выполнения;
- утечку криптографических ключей и паролей;
- утечку отдельных информационных объектов.

Приведем взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности (табл. 1),

Таблица 1.

Взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности

Угроза	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью
Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	–	+

Таблица 2.

Классификация скрытых каналов по механизму организации

Тип канала	Механизм организации канала
Параметрический пространственный	Отправитель изменяет значения наблюдаемых объектов. Получатель извлекает информацию на основании наблюдаемых значений.
Событийный пространственный	Отправитель определяет, какие из наблюдаемых объектов будут изменены. Получатель извлекает информацию путем определения наличия или отсутствия факта модификации.
Параметрический временной	Отправитель знает будущее значение наблюдаемого объекта и может управлять моментами наблюдения данного объекта получателем. С появлением необходимого значения отправитель дает возможность получателю осуществить наблюдение. Получатель извлекает информацию на основании наблюдаемых значений.
Событийный временной	Отправитель может управлять порядком изменения объектов, относительно наблюдений, осуществляемых получателем. Получатель извлекает информацию из порядка следования этих событий.

в таблице знак «+» означает, что угроза может быть реализована при наличии скрытого канала соответствующего типа; знак «–» означает, что наличие скрытого канала данного типа не может привести к реализации угрозы.

По механизму организации скрытые каналы подразделяются на четыре типа (табл.2).

Заметим, что важным является разделение на сетевые и несетевые скрытые каналы в связи с тем, что с развитием высокоскоростных сетевых технологий и возможностью негласного использования особенностей протоколов сетевого и других уровней взаимосвязи открытых систем значительно расширились возможности построения сетевых скрытых каналов и увеличились их пропускная способность. Под сетевым скрытым каналом понимается канал, в котором общий ресурс является компонентом сетевой среды.

В настоящей работе будут рассмотрены сетевые скрытые каналы, как по памяти, так и по времени. Поскольку существуют различные способы противодействия скрытым каналам путем генерации фиктивного трафика [13], увеличения длин пакетов [14], введения дополнительных случайных задержек [15], переупорядочивания пакетов [16], основное внимание будет уделено методами нормализации скрытых каналов.

1. Полная нормализация трафика как метод противодействия скрытым каналам по памяти

Пусть длины пакетов принимают значения на множестве $N_{l_{фикс}+n-1} \setminus N_{l_{фикс}-1}$, $l_{фикс}$, $n \in N$, где N_x — множество натуральных чисел, не превосходящих x. Предложен следующий способ выравнивания длин передаваемых пакетов: каждый пакет дополняется фиктивными битами до длины $l_{выр}$, если исходная длина пакета, который отправитель должен послать для передачи символа «i» не превосходит $l_{выр}$:

$$l(i) \le l_{выр}. \quad (1)$$

В противном случае пакет дополняется фиктивными битами и разбивается на минимально возможное число пакетов длины $l_{выр}$. Здесь $l_{выр}$ — параметр метода противодействия (рис. 1).

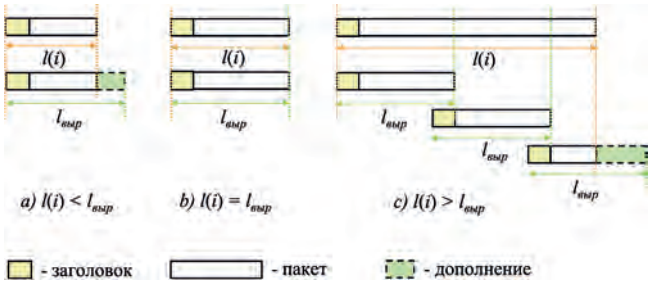

Рис. 1. Выравнивание длин передаваемых пакетов до $l_{выр}$

Рассмотрим подробнее алгоритм полной нормализации трафика. Пусть имеется исходный пакет длины $l(i) = l_{фикс} + i - 1$. Тогда:

- если $l(i) \le l_{выр}$, пакет дополняется фиктивными битами до длины $l_{выр}$;
- если $l(i) > l_{выр}$, находится минимальное число пакетов k, на которое следует разбить рассматриваемый пакет.

Выбор значения $l_{выр}$ продиктован минимизацией дополнительной нагрузки на канал связи и ограничением на максимально допустимую долю дополнительных пакетов α, где α задается владельцем канала связи.

Представим

$$l_{выр} = l_{фикс} + H, \tag{2}$$

где $l_{фикс}$ — минимально возможная длина пакета, являющаяся параметром канала связи, $H \in N_{n-1}$. Таким образом, имея распределение длин пакетов в канале связи и максимально допустимую долю дополнительных пакетов α, можно найти оптимальное значение параметра H.

Найдем дополнительную нагрузку на канал связи, заключающуюся в отправке пакетов большей длины:

$$\sum_{i=1}^{n}\left(l_{новая} - l(i)\right)p(i) = \sum_{i=1}^{n} l_{новая}\,p(i) - E(L), \tag{3}$$

где $l_{новая}$ — новая длина пакета, $p(i)$ — вероятность передачи символа «i», $E(L)$ — средняя длина пакета в трафике.

Поскольку величина $E(L)$ — константа, будем минимизировать среднюю длину новых пакетов:

$$\sum_{i=1}^{n} l_{новая}\,p(i) = \sum_{i=1}^{H+1} l_{выр}\,p(i) + \\ + \sum_{i=H+2}^{2H+1} l_{выр}\,p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kl_{выр}\,p(i). \tag{4}$$

Отсюда получаем:

$$\sum_{i=1}^{n} l_{новая}\,p(i) = (l_{вых} + H) \\ \left(\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i)\right). \tag{5}$$

Выразим ограничение, что доля дополнительных пакетов при введении противодействия не должна превышать α:

$$\frac{\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i)}{\sum_{i=1}^{n} p(i)} \le \alpha. \tag{6}$$

Отсюда получаем условие:

$$\sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i) \le \alpha. \tag{7}$$

Таким образом, решаемая задача минимизации ставится следующим образом:

$$\begin{cases} (l_{вых}+H)\left(\sum_{i=1}^{H+1} p(i)+\sum_{i=H+2}^{2H+1} 2p(i)+\ldots+\sum_{i=(k-1)H+2}^{n} kp(i)\right) \to \min\limits_{H}; \\ \sum_{i=1}^{H+1} p(i) + \sum_{i=H+2}^{2H+1} 2p(i) + \ldots + \sum_{i=(k-1)H+2}^{n} kp(i) \le \alpha. \end{cases} \tag{8}$$

Наглядно представим алгоритм нахождения оптимального значения $l_{выр}$ (рис. 2), где наилучшая длина пакета равна $l_{выр} = \min\_H + l_{фикс}$ байт, $\min\_nums$ – доля дополнительных пакетов.

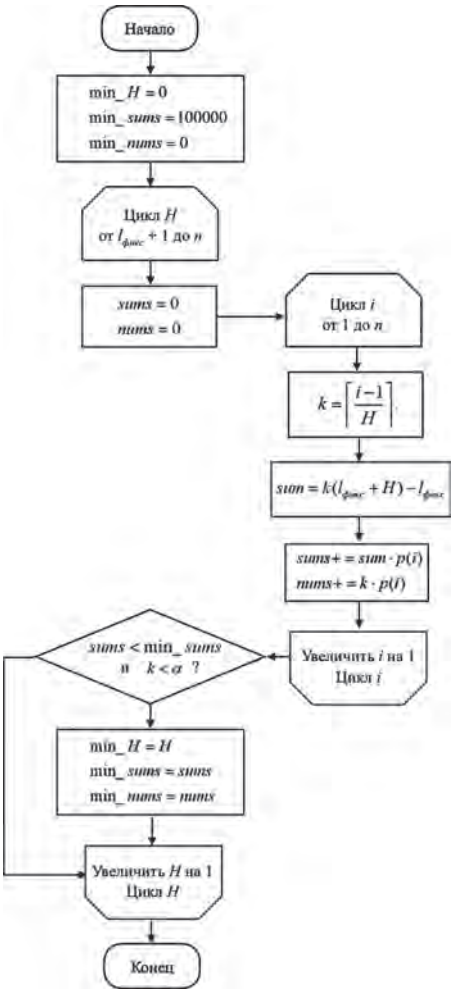

Рис. 2. Блок-схема алгоритма нахождения оптимального значения $l_{выр}$

С другой стороны, эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\frac{\beta E(L)}{(l_{вых}+H)\left(\sum_{i=1}^{H+1} p(i)+\sum_{i=H+2}^{2H+1} 2p(i)+...+\sum_{i=(k-1)H+2}^{n} kp(i)\right)}, \quad (9)$$

где β — пропускная способность канала связи.

2. Частичная нормализация трафика как метод противодействия скрытым каналам по памяти

Поскольку при полной нормализации трафика по памяти эффективная пропускная способность канала связи значительно снижается, рассмотрим частичную нормализацию трафика. При таком подходе каждый пакет дополняется фиктивными битами либо до длины $l_{выр\_1}$, либо до длины $l_{выр\_2}$, где $l_{выр\_1} = l_{фикс} + H_1$, $l_{выр\_2} = l_{фикс} + H_2$, $H_1, H_2 \in N_{n-1}$. Здесь $l_{выр\_1}$ и $l_{выр\_2}$ — параметры метода противодействия. Если длина пакета превышает $l_{выр\_2}$, то пакет дополняется фиктивными битами и разбивается на несколько пакетов с длинами $l_{выр\_1}$ и $l_{выр\_2}$.

Рассмотрим подробнее алгоритм частичной нормализации трафика (рис. 3).

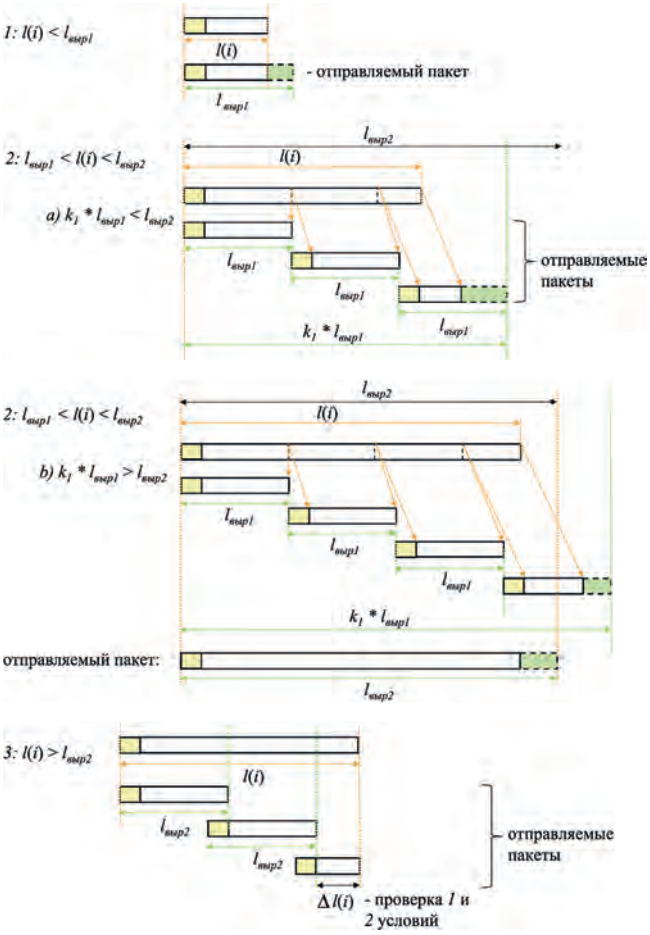

Рис. 3. Частичная нормализация трафика

Пусть имеется исходный пакет длины $l(i) = l_{фикс} + i - 1$. Тогда:

- если $l(i) \le l_{выр\_1}$, то пакет дополняется фиктивными битами до длины $l_{выр\_1}$;
- если $l_{выр\_1} < l(i) \le l_{выр\_2}$, вычисляем количество пакетов длины $l_{выр\_1}$, необходимых для отправки пакета:

$$k_1 = \left[\frac{i-1}{H_1}\right]; \quad (10)$$

- если $l_{выр\_2} \le k_1\ l_{выр\_1}$, то отправляется один пакет длины $l_{выр\_2}$;
- иначе отправляется k_1 пакетов длины $l_{выр\_1}$;
- если $l(i) > l_{выр\_2}$, то отправляется

$$k_2 = \left[\frac{i-1}{H_2}\right], \quad (11)$$

и остается нераспределенная часть пакета длиной не более $l_{выр\_2}$, поэтому повтор первых двух шагов алгоритма позволит найти искомое разбиение пакета.

Выбор параметров противодействия $l_{выр\_1}$ и $l_{выр\_2}$ производится на основе минимизации дополнительной нагрузки на канал связи и ограничением на максимально допустимую долю дополнительных пакетов α, где α задается владельцем канала связи.

Аналогично случаю полной нормализации по памяти вместо дополнительной нагрузки на канал связи найдем среднюю длину новых пакетов:

$$\sum_{i=1}^{n} l_{новая}\, p(i) = \sum_{i=1}^{n} \left\{ \left[\frac{i-1}{H_2}\right] l_{вых\_2} + \right.$$

$$\left. + \min \left\{ \frac{i - 1 - \left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1}\ l_{вых\_1},\ l_{вых\_2} \right\} \right\} p(i). \quad (12)$$

Выразим ограничение, что доля дополнительных пакетов при введении противодействия не должна превышать α:

$$\sum_{i=1}^{n} \left\{ \left[\frac{i-1}{H_2}\right] \frac{i - 1 - \left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1} \ если \right.$$

$$\left. \frac{i - 1 - \left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1}\ l_{вых\_1} < l_{вых\_2}\ иначе\ 1 \right\} p(i) \le \alpha. \quad (13)$$

Наглядно представим алгоритм нахождения оптимальных значений

$$l_{выр\_1} = min\_H_1 + l_{фикс},\ l_{выр\_2}) = min\_H_2 + l_{фикс} \quad (14)$$

и доли дополнительных пакетов $\min\_nums$ (рис. 4).

Эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\frac{\beta E(L)}{\sum_{i=1}^{n}\left\{\left[\frac{i-1}{H_2}\right] l_{вых\_2}+\min\left\{\frac{i-1-\left[\frac{i-1}{H_2}\right] l_{вых\_2}}{H_1} l_{вых\_1},\ l_{вых\_2}\right\}\right\} p(i)} \quad (14)$$

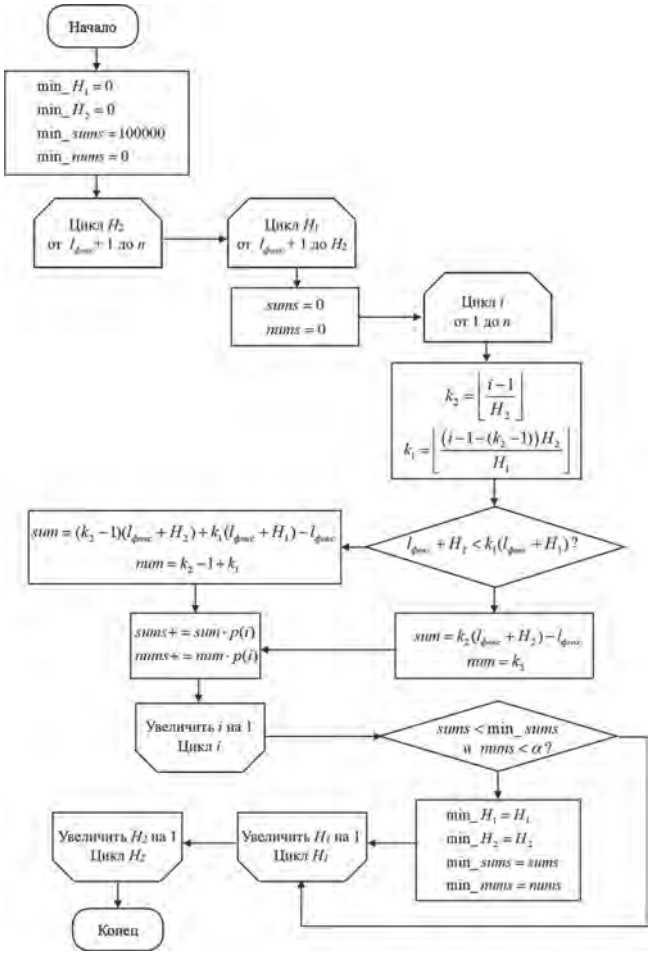

Рис. 4. Блок-схема алгоритма нахождения оптимальных значений $l_{выр\_1}$, $l_{выр\_2}$

3. Оценка остаточной пропускной способности скрытого канала по памяти при полной нормализации трафика

Для экспериментов использовались существующие данные о распределении длин пакетов протоколов IPv4 и IPv6 в трафике[3]. Были определены оптимальные значения параметра противодействия H для протоколов IPv4 и IPv6, параметр α был взят равным 2, то есть в среднем исходный пакет не должен разбиваться более чем на 2 части (табл. 3).

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. Однако если учесть, что нарушитель может построить скрытый канал по времени на основе изменения длин межпакетных интервалов, то остаточная пропускная способность скрытого канала будет приблизительно равна пропускной способности скрытого канала только по времени.

Приведем результаты оценки параметров скрытого канала по времени без ошибок (табл. 4) и с ошибками декодирования (табл. 5), в таблицах m — количество разных межпакетных интервалов, p — вероятность, с которой выбирается один из двух межпакетных интервалов в распределении Бернулли, v — пропускная способность. При исследовании параметры были выбраны следующим образом: среднее время, требуемое для передачи одного символа $\tau = 0{,}000895$ секунд, $\beta = 100$ Мбит/с.

4. Оценка остаточной пропускной способности скрытого канала при частичной нормализации трафика

При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти. Нарушителю наиболее целесообразно построить бинарный скрытый канал на основе пакетов длины $l_{фикс} + H_1$ и $l_{фикс} + H_2$. Найдем остаточную

3 Al Falasi H., Zhang L. Modeling and justification of the store and forward protocol: covert channel analysis // Proceedings of the 6th International Conference on Information Warfare and Security, 2011, p. 8.

Таблица 3.

Результаты оценки параметров метода противодействия на основе нормализации канала по памяти

	Полная нормализация			Частичная нормализация			
	$l_{выр}$, бит	Доля дополнительных пакетов	Эффективная пропускная способность /β	$l_{выр\_1}$, бит	$l_{выр\_2}$, бит	Доля дополнительных пакетов	Эффективная пропускная способность /β
IPv4	6240	1,57807	0,76619	800	12000	1,97688	0,95644
IPv6	1656	2,00000	0,75897	1152	12000	1,28330	0,94644

Таблица 4.

Пропускная способность скрытых каналов по времени без ошибок при различных распределениях

Вид распределения	Протокол сетевого уровня					
	IPv4 ($l_{вып}$ = 780 байт)			IPv6 ($l_{вып}$ = 207 байт)		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	4	—	440,78	4	-	445,28
Параболическое	5	—	491,97	4	—	497,82
Линейное	5	—	507,01	4	—	513,39
Гиперболическое	5	—	518,28	5	—	524,32
Показательное	>10	—	549,09	>10	—	556,09
Пуассона (усечённое)	>7	—	510,24	>7	—	518,45
Схема Бернулли	2	0,615237	378,31	2	0,617278	385,27

Таблица 5.

Пропускная способность скрытых каналов по времени с ошибками декодирования при различных распределениях

Вид распределения	Протокол сетевого уровня					
	IPv4 ($l_{вып}$ = 780 байт)			IPv6 ($l_{вып}$ = 207 байт)		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	4	—	784,35	4	—	800,30
Параболическое	5	—	868,51	4	—	887,94
Линейное	5	—	901,90	5	—	921,54
Гиперболическое	5	—	925,01	5	—	946,46
Показательное	>10	—	973,43	>10	—	998,13
Пуассона (усечённое)	>7	—	872,95	>7	—	900,89
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

пропускную способность полученного скрытого канала по памяти:

$$v = \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p))}{(l_{фикс}+H_1)\,p + (l_{фикс}+H_2)\,(1-p) + \beta T} =$$

$$= \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p))}{l_{фикс}+H_1+(H_2-H_1)\,(1-p)+\beta T}, \quad (15)$$

где T — длина межпакетного интервала.

Расчетным путем были найдены значение p и остаточная пропускная способность для протоколов IPv4 и IPv6 для канала без ошибок в скрытом канале только по памяти. Для протокола IPv4 пропускная способность равна 1042.24 бит/с, p = 0,520217; для протокола IPv6 пропускная способность равна 1038.53 бит/с, p = 0,519512.

Однако далее следует определить остаточную пропускную способность гибридного скрытого канала. Сначала рассмотрим скрытый канал без ошибок, то есть $T = 2\tau$. Формула пропускной способности для канала без ошибок:

$$v = \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p)) + H(T)}{(l_{фикс}+H_1)\,p + (l_{фикс}+H_2)\,(1-p) + \beta E(T)} =$$

$$= \max_p \frac{-\beta\,(p\log_2 p + (1-p)\log_2(1-p) + H(T))}{l_{фикс}+H_1+(H_2-H_1)\,(1-p)+\beta E(T)}. \quad (16)$$

Приведем зависимость остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени без ошибок, причем для каждого распределения уже выбрано оптимальное значение параметра m (рис. 5) и оценки пропускной способности (табл. 6).

Приведем зависимости остаточной пропускной способности скрытого канала от параметра p для разных значений m для шести различных распределений в гибридном скрытом канале (рис. 6).

Таблица 6.

Значения остаточной пропускной способности гибридного скрытого канала без ошибок

Вид распределения	Протокол сетевого уровня					
	IPv4			IPv6		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	2	0,5141	727,32	2	0,5136	726,42
Параболическое	3	0,5152	781,92	3	0,5147	781,09
Линейное	3	0,5156	806,79	3	0,5151	805,89
Гиперболическое	3	0,5158	813,47	3	0,5153	812,54
Показательное	>10	0,5160	824,00	>10	0,5155	823,22
Пуассона (усечённое)	>7	0,5166	855,10	>7	0,5160	854,09
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

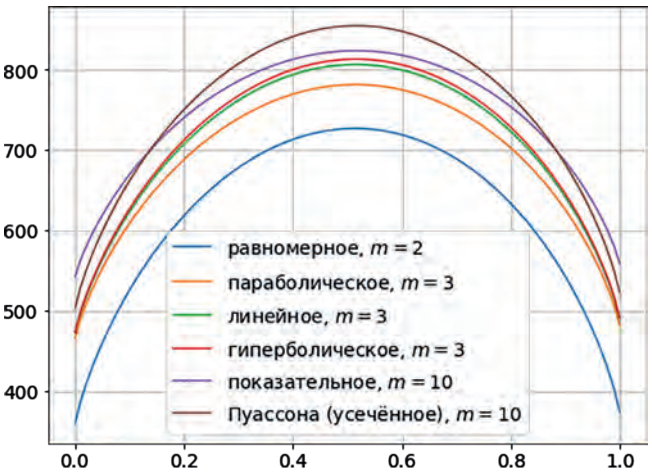

Рис. 5. График зависимости остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени без ошибок

Аналогично остаточная пропускная способность рассчитана для скрытого канала с ошибками декодирования. Приведем зависимость остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени с ошибками декодирования, отметим, что для каждого распределения выбрано оптимальное значение параметра m (рис. 7), а также результаты оценки пропускной способности для гибридного скрытого канала с ошибками декодирования для различных распределений и значений параметров m и p. (табл. 7).

Проведенные расчеты показывают, что частично нормализовать скрытые каналы по памяти не целесообразно, для такого типа скрытых каналов необходима полная нормализация.

Таблица 7.

Значения остаточной пропускной способности гибридного скрытого канала с ошибками декодирования

Вид распределения	Протокол сетевого уровня					
	IPv4			IPv6		
	m	p	v(бит/с)	m	p	v(бит/с)
Равномерное	2	0,5257	1328,77	2	0,5249	1325,51
Параболическое	3	0,5276	1425,84	3	0,5267	1422,85
Линейное	3	0,5284	1468,37	3	0,5275	1465,11
Гиперболическое	3	0,5287	1484,03	3	0,5278	1480,67
Показательное	>10	0,5293	1513,21	>10	0,5283	1510,38
Пуассона (усечённое)	>7	0,5300	1547,83	>7	0,5290	1544,21
Схема Бернулли	2	0,5972	638,43	2	0,6007	661,47

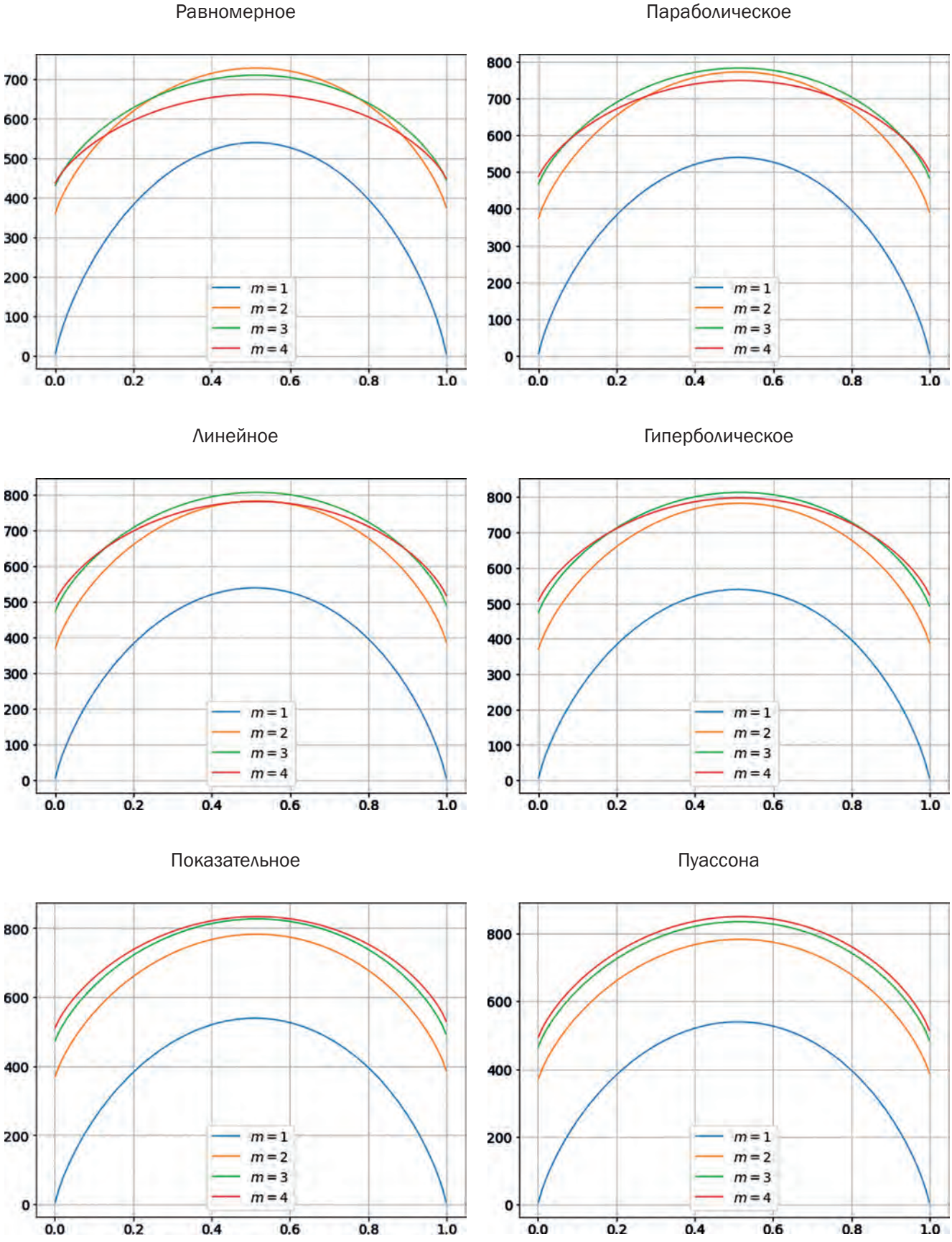

Рис. 6. Графики зависимости остаточной пропускной способности скрытого канала от параметра p для разных значений m для шести различных распределений в гибридном скрытом канале

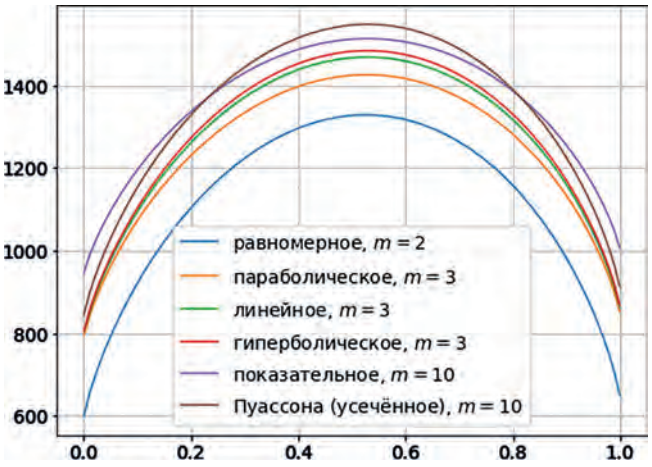

Рис. 7. График зависимости остаточной пропускной способности гибридного скрытого канала от параметра p для различных распределений в скрытом канале по времени с ошибками декодирования

5. Полная нормализация скрытого канала по времени

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. Так как в предыдущем разделе было показано, что скрытый канал по памяти необходимо полностью нормализовать, то остаточный скрытый канал может быть только скрытым каналом по времени. Соответственно, необходимо оценить возможность его нормализации.

Нормализация скрытого канала по времени осуществляется за счет введения задержек пакетов и генерации фиктивного трафика таким образом, чтобы в момент отправки между всеми пакетами были равные межпакетные интервалы $t_{выр}$. Если следующий после только что отправленного пакета пакет пришел через время $t(i) <= t_{выр}$, то этот пакет задерживается на $t_{выр} - t(i)$, и только потом отправляется. Если же пакет пришел через $t(i) > t_{выр}$, то генерируется и последовательно отравляется $[t(i) / t_{выр}] - 1$ пакетов, после чего отправляется пришедший пакет с необходимой задержкой.

При выборе параметра метода противодействия необходимо соблюдать баланс между средней задержкой пакета и объемом фиктивного трафика. Имея распределение вероятностей длин межпакетных интервалов в трафике, найдем среднюю задержку пакета d:

$$d = \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; t(i) \right) p(i). \qquad (17)$$

Доля фиктивных пакетов выражается как

$$\sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] - 1 \right) p(i) \qquad (18)$$

Пусть задан параметр γ — максимально допустимая средняя задержка пакета. Тогда для нахождения оптимального значения параметра $t_{выр}$ необходимо решить следующую задачу минимизации:

$$\begin{cases} \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] - 1 \right) p(i) \longrightarrow \min\limits_{t_{выр}}; \\ d = \sum_{i=1}^{m} \left(\left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; t(i) \right) p(i) \le \gamma. \end{cases} \qquad (19)$$

Найдем эффективную пропускную способность канала связи в условиях противодействия:

$$\beta' = \frac{E(T)}{E(T) + d} \beta = \frac{\sum_{i=1}^{m} t(i) \; p(i)}{\sum_{i=1}^{m} \left[\frac{t(i)}{t_{выр}} \right] t_{выр} \; p(i)} \beta, \qquad (20)$$

где $E(T)$ – средний межпакетный интервал в трафике.

При таком способе противодействия скрытый канал по времени полностью уничтожается. Если учесть, что длины пакетов были также выровнены, то можно прийти к выводу, что остаточная пропускная способность рассматриваемого гибридного скрытого канала стремится к нулю.

Для численной оценки параметров противодействия были проведены эксперименты с использованием данных о распределении длин межпакетных интервалов IPv4- и IPv6-пакетов, полученных из трафика[4]. При различных заданных параметрах γ расчетным путем было найдено оптимальное значение параметра $t_{выр}$, а также доля фиктивных пакетов в трафике. Также была оценена эффективная пропускная способность канала связи при значении пропускной способности канала связи $\beta = 100$ Мбит/с и при использовании значения $l_{выр}$, полученного в предыдущем подразделе (табл. 8).

Полученные результаты свидетельствуют о значительном уменьшении эффективной пропускной способности канала связи, что не позволяет применять данный метод противодействия на практике.

6. Частичная нормализация трафика как метод противодействия скрытым каналам по времени

Поскольку при полной нормализации трафика по времени эффективная пропускная способность канала связи значительно снижается, рассмотрим менее радикальный метод противодействия — частичную нормализацию трафика. При таком подходе для выравнивания используются два межпакетных интервала с длинами $t_{выр\_1}$ и $t_{выр\_2}$.

Пусть имеется исходный межпакетный интервал длиной $t(i)$. Тогда:

- если $t(i) \le t_{выр\_1}$, то пакет задерживается на $t_{выр\_1} - t(i)$ секунд;

4 https://www.caida.org/

Таблица 8.

Результаты оценки параметров метода противодействия на основе полной нормализации скрытого канала по времени

Протокол	γ, с	Средняя задержка d, с	$t_{выр}$, с	Доля фиктивных пакетов	Эффективная пропускная способность метода $/\beta$	Итоговая эффективная пропускная способность метода $/\beta$
IPv4	10^{-4}	$0{,}316 \cdot 10^{-4}$	$4{,}0055 \cdot 10^{-5}$	0	0,0499	0,0477
	10^{-5}	10^{-5}	$1{,}3829 \cdot 10^{-5}$	0,001	0,1443	0,1380
	10^{-6}	10^{-6}	$0{,}2504 \cdot 10^{-5}$	0,227	0,6269	0,5996
	10^{-7}	10^{-7}	$0{,}0338 \cdot 10^{-5}$	4,370	0,9451	0,9039
IPv6	10^{-4}	$0{,}143 \cdot 10^{-4}$	$2{,}0028 \cdot 10^{-5}$	0	0,1031	0,0976
	10^{-5}	10^{-5}	$1{,}4067 \cdot 10^{-5}$	0,001	0,1467	0,1388
	10^{-6}	10^{-6}	$0{,}2504 \cdot 10^{-5}$	0,241	0,6337	0,5997
	10^{-7}	10^{-7}	$0{,}0339 \cdot 10^{-5}$	4,355	0,9440	0,8934

- если $t_{выр\_1} < t(i) \le t_{выр\_2}$, вычисляем количество пакетов с межпакетными интервалами $t_{выр\_1}$, необходимых для того, чтобы отправить пакет через интервал $t(i)$ только с помощью длины $t_{выр\_1}$, необходимых для отправки пакета:

$$k_1 = \left[\frac{t(i)}{t_{выр\_1}} \right]; \tag{21}$$

  - если $t_{выр\_2} \le k_1 t_{выр\_1}$, то пришедший пакет задерживается на $t_{выр\_2} - t(i)$ секунд;
  - иначе отправляется $k_1 - 1$ фиктивный пакет и за ними пришедший пакет с межпакетными интервалами $t_{выр\_1}$;
- если $t(i) > t_{выр\_2}$, то отправляется

$$k_1 = \left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \tag{22}$$

фиктивный пакет с межпакетными интервалами $t_{выр\_2}$, а оставшаяся комбинация пакетов с интервалами $t_{выр\_1}$ и $t_{выр\_2}$ находится аналогично.

Выбор параметров противодействия $t_{выр\_1}$ и $t_{выр\_2}$ производится на основе минимизации доли фиктивных пакетов в трафике и ограничением на максимально допустимую среднюю задержку пакетов γ, где γ задается владельцем канала связи.

При выборе параметра метода противодействия необходимо соблюсти баланс между средней задержкой пакета и объемом фиктивного трафика. Имея распределение вероятностей длин межпакетных интервалов в трафике, найдем среднюю задержку пакета:

$$d = \sum_{i=1}^{m} \left(\left(\left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \right) t_{выр\_2} + \right.$$

$$\left. + \min \left\{ \left[\frac{t(i) - \left(\left[\frac{t(i)}{t_{выр\_2}} \right] - 1 \right) t_{выр\_2}}{t_{вых\_1}} \right] t_{вых\_1}, t_{вых\_2} \right\} - t(i) \right) p(i). \tag{23}$$

Пусть задан параметр γ — максимально допустимая средняя задержка пакета. Тогда для нахождения оптимального значения параметров $t_{выр\_1}$ и $t_{выр\_2}$ необходимо решить следующую задачу минимизации: минимизируем долю фиктивных пакетов при условии, что средняя задержка пакета не превышает γ.

Также найдем эффективную пропускную способность канала связи в условиях противодействия:

$$\beta' = \frac{E(T)}{E(T) + d} \beta . \tag{24}$$

Для численной оценки параметров противодействия были проведены эксперименты с использованием данных о распределении длин межпакетных интервалов IPv4- и IPv6-пакетов, полученных из трафика[5]. При различных заданных параметрах γ расчетным путем было найдено оптимальное значение параметров $t_{выр\_1}$ и $t_{выр\_2}$, а также доля фиктивных пакетов в трафике. Также была оценена эффективная пропускная способность канала связи при значении пропускной способности канала связи β = 100 Мбит/с и при использовании значения $l_{выр}$, полученного в предыдущем разделе (табл. 9).

7. Оценка остаточной пропускной способности скрытого канала при частичной нормализации канала по времени

После полной нормализации трафика по памяти и частичной нормализации трафика по времени у злоумышленника остается возможность построить только бинарный скрытый канал по времени на основе

5 https://www.caida.org/

Таблица 9.

Значения параметров метода противодействия на основе частичной нормализации канала по времени

	γ, с	Средняя задержка d, с	$t_{вып\_1}$, с	$t_{вып\_2}$, с	Доля фиктивных пакетов	Эффективная пропускная способность метода β' / β	Итоговая эффективная пропускная способность β' / β
IPv4	10^{-5}	$0{,}640 \cdot 10^{-5}$	$1{,}0014 \cdot 10^{-5}$	$2{,}0027 \cdot 10^{-5}$	0	0,2050	0,1937
	10^{-6}	10^{-6}	$0{,}2670 \cdot 10^{-5}$	$0{,}5027 \cdot 10^{-5}$	0,048	0,6312	0,6037
	10^{-7}	10^{-7}	$0{,}0436 \cdot 10^{-5}$	$0{,}1003 \cdot 10^{-5}$	1,106	0,9483	0,9070
IPv6	10^{-5}	10^{-5}	$1{,}4108 \cdot 10^{-5}$	$2{,}7204 \cdot 10^{-5}$	0	0,1467	0,1388
	10^{-6}	10^{-6}	$0{,}2558 \cdot 10^{-5}$	$0{,}4904 \cdot 10^{-5}$	0,068	0,6251	0,5916
	10^{-7}	10^{-7}	$0{,}0465 \cdot 10^{-5}$	$0{,}1004 \cdot 10^{-5}$	1,084	0,9473	0,8965

межпакетных интервалов $t_{вып\_1}$ и $t_{вып\_2}$. Найдем остаточную пропускную способность указанного скрытого канала по времени:

$$\nu = \max_{p} \frac{-\beta\,(p \log_2 p + (1-p) \log_2 (1-p))}{l_0 + H + (t_{вып\_1}\, p + t_{вып\_2}\, (1-p)\, \beta}. \quad (25)$$

Расчетным путем были найдены значение p и остаточная пропускная способность для протоколов IPv4 и IPv6 для канала без ошибок в скрытом канале только по памяти. Для протокола IPv4 пропускная способность равна 15843.1 бит/с, $p = 0{,}501557$; для протокола IPv6 пропускная способность равна 57826.7 бит/с, $p = 0{,}505401$. Таким образом, предложенные методы позволяют оценить целесообразность применения полной и частичной нормализации трафика для противодействия скрытым каналам по памяти и по времени.

Выводы

В работе исследованы скрытые каналы по памяти и по времени, предложены алгоритмы полной и частичной нормализации трафика для противодействия указанных скрытым каналам. Выведены формулы для оценки эффективной пропускной способности канала связи в условиях противодействия скрытым каналам и остаточной пропускной способности скрытого канала.

При полной нормализации трафика по памяти скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, полностью уничтожается в связи с тем, что все пакеты становятся одинаковой длины. Однако если учесть, что нарушитель может построить скрытый канал по времени на основе изменения длин межпакетных интервалов, то остаточная пропускная способность скрытого канала будет приблизительно равна пропускной способности скрытого канала только по времени. При частичной нормализации трафика скрытый канал по памяти, основанный на изменении длин передаваемых пакетов, уничтожается не полностью, следовательно, остается бинарный скрытый канал по памяти, оценки пропускной способности которого показывают нецелесообразность применения частичной нормализации скрытого канала по времени и указывают на необходимость его полной нормализации.

В случае, если была проведена полная нормализация длин пакетов, а остаточная пропускная способность скрытого канала все еще велика, можно дополнительно нормализовать трафик по времени. Нормализация скрытого канала по времени осуществляется за счет введения задержек пакетов и генерации фиктивного трафика таким образом, чтобы в момент отправки между всеми пакетами были равные межпакетные интервалы. В работе предложен способ противодействия, при котором скрытый канал по времени полностью уничтожается.

Рассчитаны количественные значения эффективной пропускной способности канала связи и остаточной пропускной способности скрытого канала при использовании протоколов IPv4 и IPv6, которые могут быть полезны при применении методов нормализации трафика на практике.

Литература

1. *Zhang, X., Pang, L., Guo, L., Li, Y. Building Undetectable Covert Channels Over Mobile Networks with Machine Learning // Machine Learning for Cyber Security. ML4CS 2020. Lecture Notes in Computer Science, vol 12486, 2020, pp. pp 331–339. https://doi.org/10.1007/978-3-030-62223-7_28.*
2. *Dakhane, D. M., Narawade, V. E. Reference Model Storage Covert Channel for Secure Communications // Advanced Computing Technologies and Applications. Algorithms for Intelligent Systems, 2020, pp. 489–496. https://doi.org/10.1007/978-981-15-3242-9_46.*

3. Sattolo T. A. V., Jaskolka J. Evaluation Of Statistical Tests For Detecting Storage-Based Covert Channels // IFIP Advances in Information and Communication Technology, vol. 580, 2020, pp. 17–31.
4. Dua A., Jindal V., Bedi P. Detecting And Locating Storage-Based Covert Channels In Internet Protocol Version 6 // IEEE Access, vol. 10, 2022, pp. 110661-110675.
5. Когос К. Г., Финошин М. А., Айрапетян С. В. Метод идентификации скрытых каналов по памяти в сетях пакетной передачи данных // Безопасность информационных технологий, т. 28, № 3, 2021, с. 56–64.
6. Wang, C., Chen, RL. & Gu, L. Improving Performance of Virtual Machine Covert Timing Channel Through Optimized Run-Length Encoding // Journal of Computer Science and Technology, vol. 38, 2023, pp. 793–806. https://doi.org/10.1007/s11390-021-1189-z.
7. Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.
8. Nasseralfoghara, M., Hamidi, H.R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, 2022, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.
9. Massimi, F., Benedetto, F. Performance Improvements of Covert Timing Channel Detection in the Era of Artificial Intelligence // Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol. 955, 2024, pp. pp 399–410. https://doi.org/10.1007/978-981-97-1841-2_30.
10. Zhang, Z., Zhang, X., Xue, Y., Li, Y. Building a Covert Timing Channel over VoIP via Packet Length // Data Mining and Big Data. DMBD 2021. Communications in Computer and Information Science, vol. 1453, 2021, pp. pp 81–88. https://doi.org/10.1007/978-981-16-7476-1_8.
11. Zhang, X., Guo, L., Xue, Y., Jiang, H., Liu, L., Zhang, Q. A Hybrid Covert Channel with Feedback over Mobile Networks // Security and Privacy in Social Networks and Big Data. Communications in Computer and Information Science, vol. 1095, 2019, pp. 87–94. https://doi.org/10.1007/978-981-15-0758-8_7.
12. Belozubova A., Kogos K., Epishkina A. On/Off Covert Channel Capacity Limitation by Adding Extra Delays // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 2021, pp. 2318–2322.
13. Epishkina, A., Karapetyants, N., Kogos, K. et al. Covert channel limitation via special dummy traffic generating // Journal of Computer Virology and Hacking Techniques, vol. 19, 2023, pp. 341–349. https://doi.org/10.1007/s11416-022-00428-z.
14. Epishkina, A., Frolova, D., Kogos, K. A technique to limit hybrid covert channel capacity via random increasing of packets' lengths // Procedia Computer Science, vol. 190, 2020, pp. 231–240. https://doi.org/10.1016/j.procs.2021.06.029.
15. Анна И. Белозубова, Константин Г. Когос, Филипп В. Лебедев. Ограничение пропускной способности сетевых скрытых каналов по времени путем введения дополнительных случайных задержек перед отправкой пакета // Безопасность информационных технологий, том 28, № 4, 2021, с. 74–89.
16. Gorokhov D. E., Ryabokon V. V., Kuzkin A. A., Sherbakov V. S., Kutsakin M. A. // Packet Fragmentation As Data Protection Method In Automated Systems // IOP Conference Series: Materials Science and Engineering, 2020, с. 52027.

TRAFFIC NORMALIZATION FOR INFORMATION LEAKAGE PROTECTION VIA COVERT CHANNELS

Epishkina A. V.[6], Kogos K. G.[7]

The possibility of building covert channels in an information system entails a potential leak of secured information. There are many methods of countering covert channels, but not all of them are applicable in practice. The purpose of the investigation is to develop counteraction tools to prevent information leakage via storage and timing covert channels by traffic normalization.

The authors investigate storage and timing covert channels and suggest algorithms for full and partial traffic normalization to counteract these covert channels. Using the methods of information theory, probability theory, differential and integral calculus, and data on the distribution of the lengths of inter-packet intervals of network traffic packets, formulas are derived to estimate the effective capacity of a communication channel in conditions of countering covert channels and the residual capacity of a covert channel.

When the traffic is fully normalized in memory, storage covert channel based on changing the length of transmitted packets is completely destroyed due to the fact that all packets become the same length. With partial normalization of traffic, storage covert channel, based on changing the lengths of transmitted packets, is not completely destroyed, therefore, a binary storage covert channel remains, estimates of the capacity of which show the inexpediency of using partial normalization of timing covert channel and indicate the need for its full normalization.

If full normalization of packet lengths has been carried out, and the residual capacity of the covert channel is still large, it is possible to additionally normalize traffic in time. The paper proposes a method of counteraction in which timing covert channel is completely destroyed.

Quantitative values of the effective capacity of the communication channel and the residual capacity of the covert channel when using IPv4 and IPv6 protocols are calculated, which can be useful when applying traffic normalization methods in practice.

Keywords: *information security, information leakage, counteraction tool, network covert channel, storage covert channel, timing covert channel, traffic normalization, partial normalization нормализация, channel capacity.*

6 Anna V. Epishkina, Ph.D., Associate Professor, Cryptology and Cybersecurity Department, NRNU MEPhI, Moscow, Russia. E-mail: avepishkina@mephi.ru
7 Konstantin G. Kogos, Ph.D., Associate Professor, Cryptology and Cybersecurity Department, NRNU MEPhI, Moscow, Russia. E-mail: kgkogos@mephi.ru

References

1. *Zhang, X., Pang, L., Guo, L., Li, Y. Building Undetectable Covert Channels Over Mobile Networks with Machine Learning // Machine Learning for Cyber Security. ML4CS 2020. Lecture Notes in Computer Science, vol 12486, 2020, pp. pp 331–339. https://doi.org/10.1007/978-3-030-62223-7_28.*
2. *Dakhane, D. M., Narawade, V. E. Reference Model Storage Covert Channel for Secure Communications // Advanced Computing Technologies and Applications. Algorithms for Intelligent Systems, 2020, pp. 489–496. https://doi.org/10.1007/978-981-15-3242-9_46.*
3. *Sattolo T. A. V., Jaskolka J. Evaluation Of Statistical Tests For Detecting Storage-Based Covert Channels // IFIP Advances in Information and Communication Technology, vol. 580, 2020, pp. 17–31.*
4. *Dua A., Jindal V., Bedi P. Detecting And Locating Storage-Based Covert Channels In Internet Protocol Version 6 // IEEE Access, vol. 10, 2022, pp. 110661–110675.*
5. *Kogos K. G., Finoshin M. A., Ajrapetjan S. V. Metod identifikacii skrytyh kanalov po pamjati v setjah paketnoj peredachi dannyh // Bezopasnost' informacionnyh tehnologij, t. 28, № 3, 2021, s. 56–64.*
6. *Wang, C., Chen, RL. & Gu, L. Improving Performance of Virtual Machine Covert Timing Channel Through Optimized Run-Length Encoding // Journal of Computer Science and Technology, vol. 38, 2023, pp. 793–806. https://doi.org/10.1007/s11390-021-1189-z.*
7. *Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.*
8. *Nasseralfoghara, M., Hamidi, H. R. Covert timing channels: analyzing WEB traffic // Journal of Computer Virology and Hacking Techniques, vol. 18, 2022, pp. 117–126. https://doi.org/10.1007/s11416-021-00396-w.*
9. *Massimi, F., Benedetto, F. Performance Improvements of Covert Timing Channel Detection in the Era of Artificial Intelligence // Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol. 955, 2024, pp. pp 399–410. https://doi.org/10.1007/978-981-97-1841-2_30.*
10. *Zhang, Z., Zhang, X., Xue, Y., Li, Y. Building a Covert Timing Channel over VoIP via Packet Length // Data Mining and Big Data. DMBD 2021. Communications in Computer and Information Science, vol. 1453, 2021, pp. pp 81–88. https://doi.org/10.1007/978-981-16-7476-1_8.*
11. *Zhang, X., Guo, L., Xue, Y., Jiang, H., Liu, L., Zhang, Q. A Hybrid Covert Channel with Feedback over Mobile Networks // Security and Privacy in Social Networks and Big Data. Communications in Computer and Information Science, vol. 1095, 2019, pp. 87–94. https://doi.org/10.1007/978-981-15-0758-8_7.*
12. *Belozubova A., Kogos K., Epishkina A. On/Off Covert Channel Capacity Limitation by Adding Extra Delays // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 2021, pp. 2318–2322.*
13. *Epishkina, A., Karapetyants, N., Kogos, K. et al. Covert channel limitation via special dummy traffic generating // Journal of Computer Virology and Hacking Techniques, vol. 19, 2023, pp. 341–349. https://doi.org/10.1007/s11416-022-00428-z.*
14. *Epishkina, A., Frolova, D., Kogos, K. A technique to limit hybrid covert channel capacity via random increasing of packets' lengths // Procedia Computer Science, vol. 190, 2020, pp. 231–240. https://doi.org/10.1016/j.procs.2021.06.029.*
15. *Anna I. Belozubova, Konstantin G. Kogos, Filipp V. Lebedev. Ogranichenie propusknoj sposobnosti setevyh skrytyh kanalov po vremeni putem vvedenija dopolnitel'nyh sluchajnyh zaderzhek pered otpravkoj paketa // Bezopasnost' informacionnyh tehnologij, tom 28, № 4, 2021, s. 74–89.*
16. *Gorokhov D. E., Ryabokon V. V., Kuzkin A. A., Sherbakov V. S., Kutsakin M. A. // Packet Fragmentation As Data Protection Method In Automated Systems // IOP Conference Series: Materials Science and Engineering, 2020, c. 52027.*