ВЕСТНИК НАЦИОНАЛЬНОГО ИССЛЕДОВАТЕЛЬСКОГО ЯДЕРНОГО УНИВЕРСИТЕТА “МИФИ”, 2021, том 10, № 4, с. 349–356

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

УДК 519.688

ИМИТАЦИЯ DDoS-АТАКИ В МАГИСТРАЛЬНОМ КАНАЛЕ

© 2021 г. В. В. Иванов[1], В. В. Иванов[1,2], А. В. Крянев[2,*], А. С. Приказчикова[2], И. И. Татаринов[1,3]

[1] Объединенный институт ядерных исследований, Дубна, 141980, Россия

[2] Национальный исследовательский ядерный университет “МИФИ”, Москва, 115409, Россия

[3] АО “Лаборатория Касперского”, Москва, 125212, Россия

**e-mail: AVKryanev@mephi.ru*

Поступила в редакцию 12.08.2021 г.
После доработки 16.08.2021 г.
Принята к публикации 24.08.2021 г.

Ранее нами было показано, что при агрегации измерений сетевого трафика, начиная с определенного размера окна агрегации, формируется стабильное распределение, которое с высокой точностью аппроксимируется логнормальным законом. Кроме того, нами наблюдалось нарушение этого закона в процессе вредоносной атаки на локальную сеть небольшого размера. В настоящей работе обсуждается процедура организации DDoS-атаки с помощью изменения интернет-трафика, зарегистрированного на магистральном канале. В результате проведенных исследований было установлено, что при имитации DDoS-атаки не наблюдается разрушения логнормального закона. Поэтому для проверки факта разрушения логнормального закона при вредоносной атаке на сеть необходима организация контролируемой DDoS-атаки на конкретный сетевой ресурс.

Ключевые слова: сетевой трафик, сетевой ресурс, окно агрегации, логнормальное распределение, DDoS-атака, магистральный канал, контролируемая DDoS-атака

DOI: 10.1134/S2304487X21040052

ВВЕДЕНИЕ

Ранее в работе [1] нами было показано, что также, как для локальной сети среднего размера [2, 3], при агрегировании измерений интернет-трафика в магистральном канале формируются статистические распределения, которые с высокой точностью аппроксимируются суммой логнормальных распределений [4].

Следует отметить, что несмотря на то, что в установившемся режиме при определенном уровне агрегации основное распределение информационного потока отвечает логнормальному закону, возможны изменения сетевой среды, связанные, в частности, с изменением активности пользователей, которые могут привести либо к подобным состояниям, но с другими параметрами логнормального распределения, либо к переходным режимам, распределения информационного потока в которых не следуют логнормальному закону (например, при перегрузках, или же в случае проведения вредоносных атак на сетевую инфраструктуру) [5].

Для наблюдения за динамикой информационных потоков нами были разработаны методы для фиксации моментов смены состояний анализируемых временных рядов [6]. В основу этих методов положена гипотеза о том, что основное состояние информационного потока должно следовать логнормальному закону.

Развитые методы были впервые успешно применены при анализе реальных измерений (включая, в том числе, проведение вредоносной атаки), зарегистрированных на входном шлюзе локальной сети университета “Дубна” [5, 6].

Определенный интерес представляют измерения, связанные с проведением вредоносной атаки: начало атаки, ее динамика и окончание.

Детальный анализ указанных данных, исследование их особенностей может позволить разработать программные и технические средства для предотвращения серьезных последствий от воздействия вредоносных атак на сетевые ресурсы.

С учетом того, что организация и проведение вредоносной атаки на локальную сеть и/или на конкретный сетевой ресурс, может приводить к порой непредсказуемым или разрушительным последствиям, нами была исследована возможность имитации DDoS-атаки используя только данные интернет-трафика, которые были получены ранее в измерениях на магистральном канале [7].

1. DDoS-АТАКА

DDoS-атака (англ. *Distributed Denial of Service*) переводится как “отказ от обслуживания”. Это вредоносная атака на вычислительную или сетевую систему с целью выведения ее из строя путем организации большого количества обманных запросов. При этом серверам приходится обрабатывать объем запросов, значительно превышающий возможности атакованного сайта. В результате, легальные пользователи не могут получить доступ к предоставляемым сетевым ресурсам, либо этот доступ будет сильно затруднен [8].

Один из способов DDoS-атаки – это насыщение полосы пропускания большими объемами данных, что приводит к:

1) потере сетевых пакетов при передаче между легальными клиентами и атакованным сервером;

2) сбоям при обработке запросов от легальных клиентов в связи с максимальной загрузкой сетевого оборудования.

Эффект от DDoS-атаки, связанной с насыщением полосы пропускания, т.е. нарушение работоспособности атакованного сервера, наступает зачастую лишь через значительное время от начала атаки. Поэтому своевременное обнаружение DDoS-атак может позволить эффективно им противодействовать и свести к минимуму вред, причиняемый такими атаками.

Ранее нами было показано, что плотность вероятности распределения (ПВР) интенсивности сетевого трафика, характеризующая процесс передачи данных в сети, и ПВР скорости передачи сетевых пакетов, характеризующая стабильность работы сетевого оборудования, с высокой точностью аппроксимируются логнормальным законом [4].

Поэтому одним из подходов по обнаружению DDoS-атаки до момента нарушения работоспособности сетевого оборудования может служить мониторинг характеристик сетевого трафика. В этой связи, можно предположить, что “разрушение” логнормального закона, которым аппроксимируются соответствующие ПВР, может быть указанием на то, что происходит несанкционированное вмешательство в сетевой трафик и/или в работу сетевого оборудования. Следует отметить, что указанный эффект наблюдался нами ранее в процессе имитации вредоносной атаки на локальную сеть университета “Дубна” [5, 6].

Для проверки указанной гипотезы требуется выполнить контролируемую DDoS-атаку на конкретный сервер, собрать данные о сетевом трафике, попытаться выделить из трафика DDoS-атаку и провести ее детальный анализ. К сожалению, такой подход требует значительных затрат времени и вычислительных ресурсов. Поэтому можно попытаться решить эту проблему более простым, но менее надежным способом. А именно, смоделировать DDoS-атаку, сформировав ее из ранее полученного сетевого трафика при обычной работе сетевого канала и сетевого трафика, свойственного сети, подвергшейся DDoS-атаке.

2. ИМИТАЦИЯ DDoS-АТАКИ

Сетевой трафик обычно включает интервалы времени, в течение которых интенсивность сетевого трафика и/или скорость передачи сетевых пакетов могут существенно превышать текущие средние показатели, достигая порой уровня максимальной пропускной способности сетевого канала и/или максимальной производительности сетевого оборудования.

Следует отметить, что в такие моменты ситуация близка к той, которая возникает при DDoS-атаке, но поскольку она длится значительно меньше времени, чем реальная атака, то оборудование успешно справляется с возникшей перегрузкой: сетевое оборудование обычно имеет некоторый “запас прочности”, что позволяет выдерживать кратковременное увеличение интенсивности сетевого трафика и/или запросов к оборудованию (или же пользователи не успевают заметить возникших со связью проблем).

Поэтому для имитации DDoS-атаки необходимо сформировать новый трафик, в котором интенсивность и/или скорость передачи сетевых пакетов должны длительное время находиться на уровне максимальной пропускной способности сетевого канала и/или максимальной производительности сетевого оборудования. Выбирая пакеты сетевого трафика из указанных интервалов можно попытаться сформировать такой трафик, который будет имитировать DDoS-атаку за счет насыщения канала данными и/или сетевого оборудования запросами.

При этом следует искать компромисс между длительностью интервалов времени, из которых выбираются сетевые пакеты, и интенсивностью сетевого трафика, поскольку имеет место следующая закономерность:

– чем больше интервал времени, из которого выбираются сетевые пакеты, тем более длительный эффект оказывается на сетевое оборудование, что, в свою очередь, вызывает больший отклик сетевого оборудования, схожий с откликом на DDoS-атаку;

– но при этом, чем больше интервал времени, из которого выбираются сетевые пакеты, тем ниже интенсивность сетевого трафика для указанного интервала времени, что, соответственно, вызывает меньший отклик сетевого оборудования, схожий с откликом на DDoS-атаку;

– чем выше интенсивность сетевого трафика в выбранном интервале времени, тем более силь-

ный эффект оказывается на сетевое оборудование, что, в свою очередь, вызывает больший отклик сетевого оборудования, схожий с откликом на DDoS-атаку;

– но при этом, чем выше интенсивность сетевого трафика в выбранном интервале времени, тем менее длительный эффект оказывается на сетевое оборудование, что, в свою очередь, вызывает меньший отклик сетевого оборудования, схожий с откликом на DDoS-атаку;

– чем меньше интервалы времени, из которых выбираются сетевые пакеты, тем меньше суммарная длительность формируемого сетевого трафика и тем больше погрешности при формировании ПВР интенсивности сетевого трафика.

С учетом вышесказанного, процедура формирования сетевого трафика, имитирующего DDoS-атаку, заключалась в следующем:

1) из измерений реального сетевого трафика, взятых на сайте [7], извлекается ПВР интенсивности для заданного типа сетевых пакетов и режима их передачи;

2) используя извлеченное ПВР определяется максимальная интенсивность $I_{\max}$, которой в сетевом трафике должен соответствовать примерно 1% сетевых пакетов: (имитация насыщения сетевого канала данными);

3) измерения реального сетевого трафика агрегируются с разными окнами (1 с, 2 с, 10 с) и для каждого варианта вычисляются соответствующие интенсивности I_{local};

4) из измерений реального трафика отбираются последовательности сетевых пакетов, для которых вычисленная интенсивность I_{local} превышает максимальную $I_{\max}$;

5) из отобранных последовательностей формируется новый сетевой трафик, в котором корректируется время получения сетевых пакетов (проводится, так называемая, “склейка” сетевых пакетов):

a. для каждой из отобранных последовательностей сохраняются интервалы между сетевыми пакетами;

b. интервал между последовательными пакетами соседних последовательностей (т.е. интервал между последним сетевым пакетом предыдущей последовательности и первым сетевым пакетом последующей последовательности) устанавливается таким, чтобы полученная интенсивность превосходила интенсивность $I_{\max}$.

Аналогичная процедура по формированию нового сетевого трафика, имитирующего DDoS-атаку, использовалась для ПВР скорости передачи сетевых пакетов.

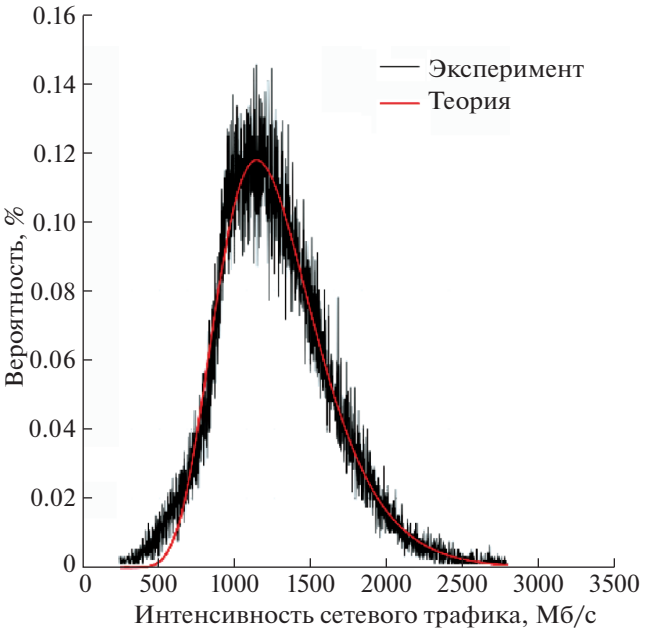

Рис. 1. Аппроксимация логнормальным распределением ПВР интенсивности трафика, имитирующего DDoS-атаку: регистрация всех сетевых пакетов в дуплексном режиме (ширина окна агрегации 1 мс).

3. АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Подготовленные в соответствии с описанной выше процедурой ПВР интенсивности сетевого трафика и ПВР скорости передачи сетевых пакетов использовались для имитации симплексного и дуплексного режимов работы при передаче: 1) всех сетевых пакетов, 2) только TCP пакетов, 3) только служебных пакетов.

При этом проверялось соответствие вновь сформированных ПВР логнормальному закону, а также анализировались различия между ПВР, подготовленных на основе реального трафика, и ПВР, подготовленных для трафика, имитирующего DDoS-атаку.

3.1. ПВР сетевого трафика, имитирующего DDoS-атаку

Из рисунков 1–4 видно, что ПВР, сформированные на основе трафика, имитирующего DDoS-атаку, хорошо аппроксимируются логнормальным распределением как для всех сетевых пакетов (которые содержат в основном TCP пакеты): рис. 1 и рис. 2, так и для служебных пакетов: рис. 3 и рис. 4.

При этом мы не заметили каких-либо существенных расхождений между реальным сетевым трафиком и трафиком, имитирующим DDoS атаку: в обоих случаях распределения ПВР с высокой точностью аппроксимируются логнормальным законом.

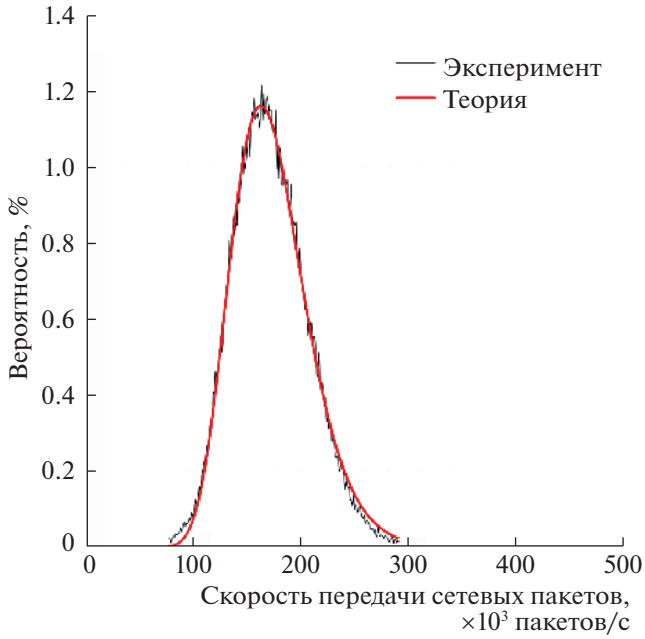

Рис. 2. Аппроксимация логнормальным распределением ПВР скорости передачи сетевых пакетов трафика, имитирующего DDoS-атаку: регистрация всех сетевых пакетов в дуплексном режиме (ширина окна агрегации 1 мс).

При сравнении ПВР интенсивности трафика для всех сетевых пакетов (рис. 1) с ПВР интенсивностью трафика только для служебных пакетов (рис. 3), следует отметить сильный разброс интенсивности у последнего ПВР по сравнению с первым. Это связано с тем, что вклад служебных пакетов в реальный сетевой трафик составляет менее 1%. Кроме того, из всех служебных пакетов отбирались только такие, которые удовлетворяли критериям, описанным в разделе 2. В результате, чем меньшее количество пакетов включает анализируемый сетевой трафик, тем большие разбросы интенсивностей возникают при формировании соответствующей ПВР.

Следует также отметить, что для одних и тех же типов сетевых пакетов и способов их передачи для ПВР скорости передачи сетевых пакетов (рис. 3 и рис. 4) наблюдается более стабильное поведение для ПВР интенсивности сетевого трафика (рис. 1 и рис. 2). Очевидно, что это вызвано тем, что ПВР скорости передачи сетевых пакетов зависит только от интервалов времени между соседними сетевыми пакетами, в то время как ПВР интенсивности сетевого трафика содержит различные пакеты, размеры которых колеблются в больших диапазонах значений.

3.2. Отличия ПВР трафика, имитирующего DDoS-атаку, от реального трафика

Сравнение ПВР интенсивности реального сетевого трафика с ПВР интенсивности сетевого трафика, имитирующего DDoS-атаку, позволяет выделить два основных отличия:

– максимум ПВР интенсивности трафика, имитирующего DDoS-атаку, сильно смещен в сторону высоких скоростей (рис. 9), что ожидае-

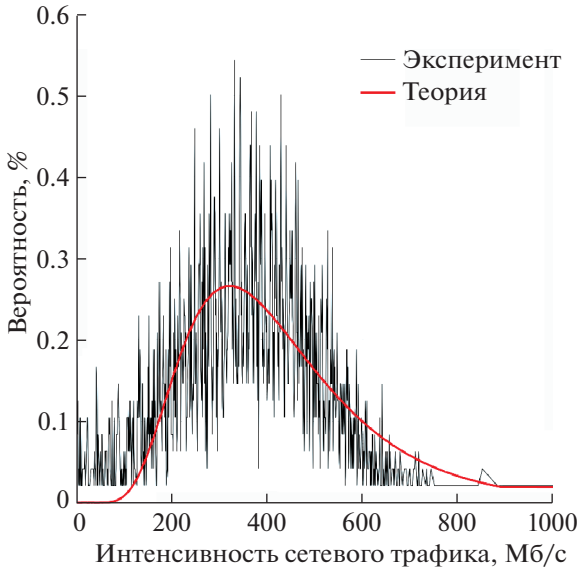

Рис. 3. Аппроксимация логнормальным распределением ПВР скорости передачи сетевых пакетов трафика, имитирующего DDoS-атаку: регистрация служебных сетевых пакетов в симплексном режиме (ширина окна агрегации 1 мс).

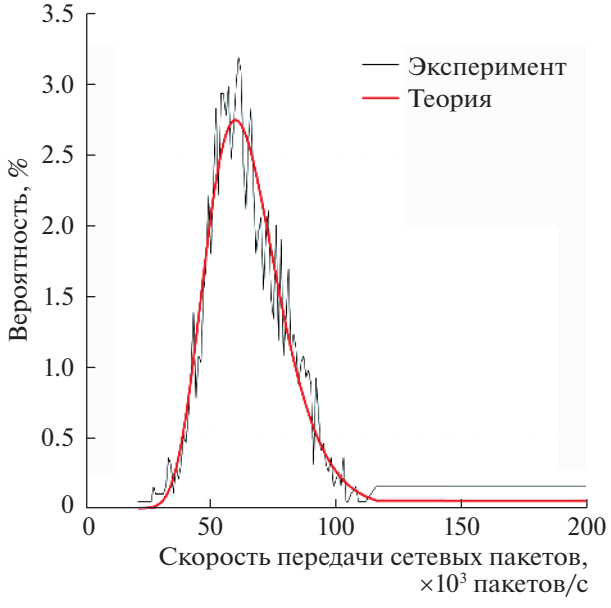

Рис. 4. Аппроксимация логнормальным распределением ПВР скорости передачи сетевых пакетов трафика, имитирующего DDoS-атаку: регистрация служебных сетевых пакетов в симплексном режиме (ширина окна агрегации 10 мс).

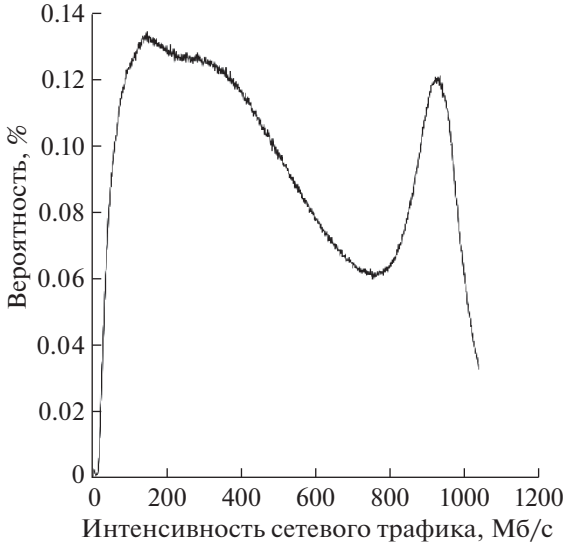

Рис. 5. ПВР интенсивности сетевого трафика для всех сетевых пакетов, зарегистрированных в дуплексном режиме (ширина окна агрегации 1 мс).

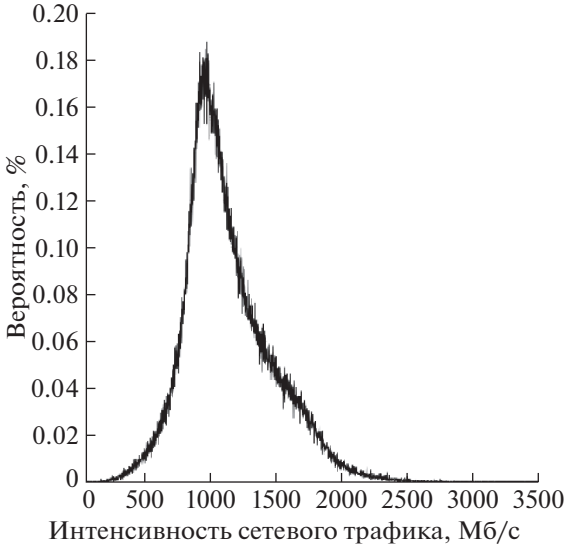

Рис. 6. ПВР интенсивности трафика, имитирующего DDoS-атаку, для всех сетевых пакетов, зарегистрированных в дуплексном режиме (ширина окна агрегации 1 мс).

мо, поскольку из реального сетевого трафика выбирались последовательности сетевых пакетов с высокой интенсивностью (99% от пиковой) (смотри раздел 2);

– для сетевых пакетов, передаваемых в дуплексном режиме, у ПВР интенсивности трафика, имитирующего DDoS-атаку (рис. 6), исчезает, или же становится слабо выраженным второй пик, который был ярко выражен в ПВР интенсивности для реального сетевого трафика (рис. 5).

Аналогичное поведение наблюдается и для ПВР скорости передачи сетевых пакетов (рис. 7, рис. 8 и рис. 10).

ПВР интенсивности для реального трафика и трафика, имитирующего DDoS-атаку (рис. 9), и ПВР скорости передачи сетевых пакетов для реального трафика и для трафика, имитирующего DDoS-атаку (рис. 10), имеют разные значения максимумов. Это обусловлено тем, что пики ПВР для реального трафика уже пиков для трафика, имитирующего DDoS-атаки (на указанных рисунках используется логарифмическая школа, поэтому разность ширин не очень заметна), а поскольку площадь ПВР одинаковая (и равна 100%), то это сказывается на значениях максимумов.

4. АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ И ВЫВОДЫ

В результате проведенной работы нами получены следующие результаты:

1) ПВР интенсивности сетевого трафика и ПВР скорости передачи сетевых пакетов для реального трафика и для трафика, имитирующего DDoS-атаку, с высокой точностью аппроксимируются логнормальным законом: не наблюдается предполагаемого “разрушения” логнормального закона;

2) ПВР скорости передачи сетевых пакетов, характеризующие работу сетевого оборудования, намного точнее, по сравнению с ПВР интенсивности сетевого трафика, фитируются логнормальным распределением, как для реального тра-

Рис. 7. ПВР скорости передачи сетевых пакетов для всех сетевых пакетов, зарегистрированных в дуплексном режиме (ширина окна агрегации 1 мс).

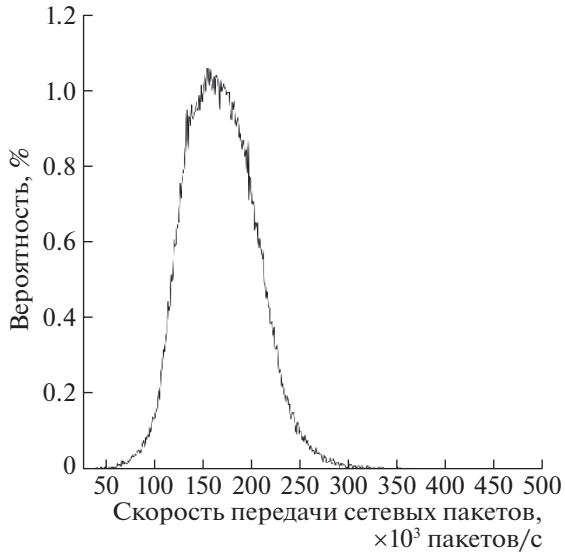

Рис. 8. ПВР скорости передачи сетевых пакетов трафика, имитирующего DDoS-атаку, для всех сетевых пакетов, зарегистрированных в дуплексном режиме (ширина окна агрегации 1 мс).

фика, так и для трафика, имитирующего DDoS-атаку;

3) В ПВР интенсивности сетевого трафика и ПВР скорости передачи сетевых пакетов для трафика, имитирующего DDoS-атаку в дуплексном режиме, практически исчезает второй пик, отчетливо наблюдаемый в ПВР для измерений реального трафика.

Анализ полученных результатов позволяет сделать следующие выводы:

– Так как увеличение интенсивности трафика не оказывает негативного воздействия на логнормальный закон, которым аппроксимируется ПВР интенсивности сетевого трафика, то можно предположить, что пропускная способность магистрального канала превышает имитируемую интенсивность сетевого трафика;

– ПВР скорости передачи сетевых пакетов аппроксимируется логнормальным законом как при низкой, так и при высокой интенсивностях трафика. Поскольку ПВР скорости передачи сетевых пакетов характеризует работу сетевого оборудования, то можно сделать вывод о том, что сетевое оборудование надежно работает как при средних нагрузках, так и при непродолжительных высоких нагрузках;

– Подавление второго пика в ПВР интенсивности сетевого трафика и ПВР скорости передачи сетевых пакетов в дуплексном режиме вероятнее всего носит искусственный характер. Дело в том, что сетевые пакеты, регистрируемые в дуплексном режиме, можно разбить две группы: 1) включает последовательные пакеты, интервалы между которыми превышают 1 мкс, 2) содержит пакеты с интервалами менее 1 мкс. При формировании сетевого трафика, имитирующего DDoS-атаку, в процессе отбора из реального трафика сетевых пакетов с высокой интенсивностью естественным образом отбрасываются пакеты, относящиеся к первой группе.

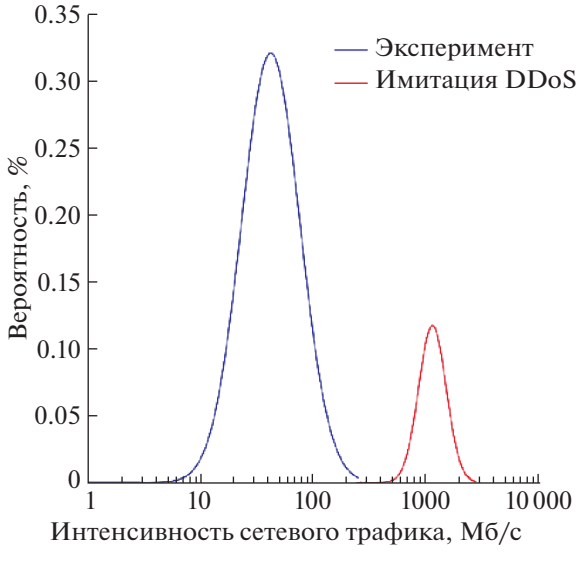

Рис. 9. Аппроксимация ПВР интенсивности реального трафика и трафика, имитирующего DDoS-атаку, для TCP сетевых пакетов, зарегистрированных в симплексном режиме (ширина окна агрегации 1 мс).

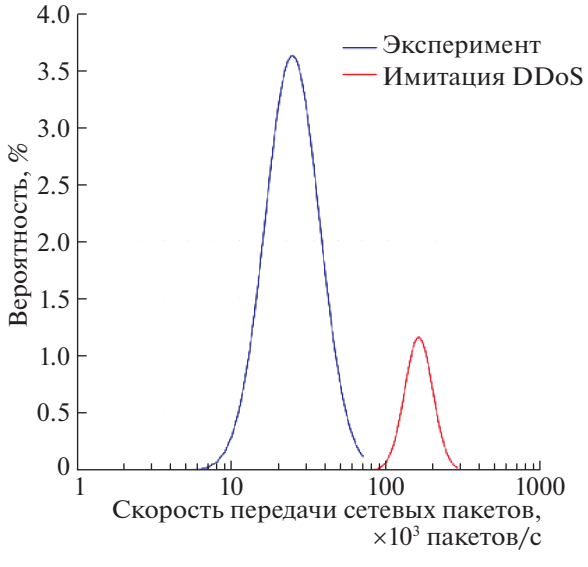

Рис. 10. Аппроксимация ПВР скорости передачи сетевых пакетов реального трафика и трафика, имитирующего DDoS-атаку, для TCP сетевых пакетов, зарегистрированных в симплексном режиме (ширина окна агрегации 1 мсек).

Результаты проведенных исследований позволяют констатировать, что имитация DDoS-атаки не позволила достичь ожидаемого результата, а именно, “разрушения” логнормального закона в процессе имитации атаки на сетевой ресурс. В этой связи, для детального анализа динамики сетевого трафика при DDoS-атаке на сетевой ресурс необходима организация реальной (хотя и контролируемой) атаки на конкретный сетевой ресурс.

СПИСОК ЛИТЕРАТУРЫ

1. *Zrelov P.V., Ivanov V.V., Ivanov V.V., Kryukov Yu.A., Tatarinov I.I.* Study of Internet-Traffic Features in the Trunk Channel // Physics of Particles and Nuclei Letters. 2019. V. 16. № 3. P. 289–299.
2. *Antoniou I., Ivanov V.V., Ivanov V.V., Zrelov P.V.* On the Log-Normal Distribution of Network Traffic // Physica D: Nonlinear Phenomena. 2002. V. 167. P. 72–85.
3. *Antoniou I., Ivanov V.V., Ivanov V.V., Zrelov P.V.* Statistical Model of Network Traffic // Физика элементарных частиц и атомного ядра (ЭЧАЯ). 2004. Т. 35. Вып. 4. С. 984–1019.
4. *Иванов В.В., Иванов В.В., Крянев А.В., Татаринов И.И.* Аппроксимация измерений интернет-трафика в магистральном канале суммой логнормальных распределений // Вестник НИЯУ “МИФИ”. 2019. Т. 8. № 4. С. 380–394.
5. *Иванов В.В.* Статистическая модель информационного трафика: Автореферат дисс. ... канд. физ.-мат. наук. Дубна, 2009.
6. *Ivanov V.V., Ivanov V.V., Kryukov Yu.A., Zrelov P.V.* Detection of Abrupt Changes in Network Trafic Dynamics, In: Annual report 2004–2005 years. Laboratory of Information Technologies. Ed. by Gh. Adam, V.V. Ivanov and T.A. Strizh, JINR, 2005-179, Dubna. 2005. P. 66–72.
7. MAWI Working Group Traffic Archive. [Электронный ресурс]. URL: http://mawi.wide.ad.jp/mawi/ (дата обращения: 18.01.2020).
8. *Dittrich D., Mirkovic J., Reiher P., Dietrich* S. Internet Denial of Service: Attack and Defense Mechanisms. Москва. Pearson Education, 2004. С. 400. ISBN 0132704544, 9780132704540.

Vestnik Natsional’nogo issledovatel’skogo yadernogo universiteta “MIFI”, 2021, vol. 10, no. 4, pp. 349–356

Simulation of a DDoS Attack in the Trunk Channel

V. V. Ivanov[a], V. V. Ivanov[a,b], A. V. Kryanev[b,#], A. S. Prikazchikova[b], and I. I. Tatarinov[a,c]

[a] *Joint Institute for Nuclear Research, Dubna, Moscow oblast, 141980 Russia*

[b] *National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, 115409 Russia*

[c] *Kaspersky Lab, Moscow, 125212 Russia*

[#] *e-mail: AVKryanev@mephi.ru*

Received August 12, 2021; revised August 16, 2021; accepted August 24, 2021

Abstract—Earlier, we showed that when aggregating network traffic measurements, starting from a certain aggregation window, a stable distribution is formed, which is approximated with a high accuracy by a lognormal law. In addition, we observed a violation of this law during a hacker attack on a small local area network. The procedure for organizing a DDoS attack using measurements of Internet traffic, recorded in the trunk channel is discussed in this work. It has been found that when simulating a DDoS attack, no violation of the lognormal law is observed. Therefore, to verify the deviation from the lognormal law in a hacker attack on a network, it is necessary to organize a controlled DDoS attack on a specific network resource.

Keywords: network traffic, network resource, aggregation window, lognormal distribution, DDoS attack, backbone, controlled DDoS attack

DOI: 10.1134/S2304487X21040052

REFERENCES

1. Zrelov P.V., Ivanov Valery V., Ivanov Victor V., Kryukov Yu. A., Tatarinov I.I.. Study of Internet-Traffic Features in the Trunk Channel, *Physics of Particles and Nuclei Letters*, 2019, vol. 16, no. 3. P. 289–299.
2. Antoniou I., Ivanov V.V., Ivanov Valery V., and Zrelov P.V. On the Log-Normal Distribution of Network

Traffic, *Physica D. Nonlinear Phenomena*., 2002, vol. 167, pp. 72–85.

3. Antoniou I., Ivanov V.V., Ivanov Valery V., and Zrelov P.V. Statistical Model of Network Traffic, Fizika elementarnih chastits i atomnogo yadra. (FEChAYa), 2004, vol. 35, no. 4. P. 984–1019.
4. Ivanov V.V., Ivanov V.V., Kryanev A.V., Tatarinov I.I., Appraksimatsita izmerenii internet-trafika v magistralnom kanale cummoi lognormal"nih raspredelenii, Vestnik "MEPhI", 2019, vol. 8, no. 4. P. 380–394.
5. Ivanov V.V. Statisticheskaya model' informacionnogo trafika. Avtoref. Diss. kand. Phiz.-math. nauk .[Statistical model of information traffic. Avtoref. Dr. phys. and math. sci. diss.], Dubna, 2009.
6. Ivanov V.V., Ivanov Valery V., Kryukov Yu. A. and Zrelov P.V. Detection of Abrupt Changes in Network Traffic Dynamics. *Annual report 2004–2005 years. Laboratory of Information Technologies.* Ed. by Adam Gh., Ivanov V.V. and Strizh T.A., JINR, 2005–179, Dubna, 2005. P. 66–72.
7. *MAWI Working Group Traffic Archive.* URL: http://mawi.wide.ad.jp/mawi//.(accessed 18.01.2020)
8. Dittrich D., Mirkovic J., Reiher P., Dietrich S.. *Internet Denial of Service: Attack and Defense Mechanisms.* Moscow, Pearson Education Publ., 2004, p. 400, ISBN 0132704544, 9780132704540.