Для цитирования: Жарова О.Ю. Применение системы анализа сетевой нагрузки для выявления начала DDoS -атаки // Вопросы радиоэлектроники. 2018. № 11. С. 48–52.
DOI 10.21778/2218-5453-2018-11-48-52
УДК 004.7.056

О.Ю. Жарова[1]

[1] Московский государственный технический университет им. Н.Э. Баумана, Калужский филиал

ПРИМЕНЕНИЕ СИСТЕМЫ АНАЛИЗА СЕТЕВОЙ НАГРУЗКИ ДЛЯ ВЫЯВЛЕНИЯ НАЧАЛА DDOS-АТАКИ

При работе различных веб-ресурсов, в том числе государственных площадок и геоинформационных систем, существует проблема атак на отказ в обслуживании (Distributed Denial of Service – DDoS-атак). Целью данного исследования является определение эффективности разработанной системы анализа сетевой нагрузки. Рассматривается проблема DDoS-атак, а также существующие методы и меры противодействия атакам данного вида. Подробно рассмотрен подход к определению факта начала атаки. Описывается разработанная система, ее архитектура и функционал каждого модуля. Приводятся результаты тестирования в условиях нормального трафика и резко возрастающей нагрузки, моделирующей ситуацию лавинообразной DDoS-атаки. Для визуализации процесса мониторинга система строит графики, на которых отчетливо видно начало атаки. Сделан вывод, что система может быть использована для выявления DDoS-атак.

Ключевые слова: *атака на отказ в обслуживании, статистические параметры, трафик*

Введение

Постоянные статистические сводки свидетельствуют о том, что проблема DDoS-атак (Distributed Denial of Service – отказ от обслуживания), как и 10 лет назад, не теряет своей актуальности. По данным публикуемого ежеквартального отчета DDoS Intelligence (система DDoS Intelligence является частью решения Kaspersky DDoS Protection), можно судить о том, что активность бот-нетов то растет, то незначительно снижается, изменяется процентное соотношение жертв в различных странах мира. Так называемая первая десятка – список стран с самой высоким количеством целей DDoS-атак на их территориях – может варьироваться от года к году, что зачастую зависит от политических и экономических ситуаций в этих странах. В последние три года количество DDoS-атак выросло. Динамика увеличения значительно сократилась, но тенденция осталась. С учетом роста компьютеризации социума и перехода большого количества услуг и сервисов в интернет-формат ущерб, наносимый такого рода атаками, постоянно растет [1].

Меры и методы противодействия DDoS-атакам

Методы защиты от DDoS-атак можно разделить на две группы: противодействующие, которые применяют, чтобы предотвратить атаку как таковую; методы активной защиты, которые применяют непосредственно после начала атаки для противодействия DDoS-трафику, а также для смягчения результатов атаки [2].

К группе методов по предотвращению атак можно отнести организационно-правовые мероприятия, устранение уязвимостей и поддержку задействованного аппаратно-программного комплекса в актуальном состоянии. Существуют виды DDoS-атак, направленных именно на эксплуатацию различного рода уязвимостей. Это могут быть как уязвимости в программном обеспечении сервера, так и уязвимости, связанные с использованием неоптимизированных программных скриптов (например, поиск по сайту), которые могут чрезмерно расходовать ресурсы сервера даже при невысокой интенсификации запросов.

После начала атаки применяются активные меры, направленные на противодействие атаке, такие как наращивание ресурсов и фильтрация трафика.

Для эффективных мер противодействия и фильтрации трафика необходимо решение двух тесно связанных задач. Первая задача заключается в обнаружении факта начала атаки, вторая – в определении источника атаки, т.е. источника вредоносного трафика. Чем точнее будут решены эти задачи, тем эффективнее будут меры противодействия. На сегодняшний день существует несколько подходов, связанных с определением начала атаки, но одним из самых перспективных можно считать подход, основанный на анализе аномалий. Обнаружение атаки происходит путем сопоставления текущего состояния системы с ее нормальным состоянием.

В результате работы системы противодействия DDoS-атаке должны осуществляться постоянный сбор данных, характеризующих состояние системы, их обработка и анализ на предмет отличия от модельных данных (рис. 1). В случае начала атаки задействуются механизмы обнаружения источника трафика.

Разработанная система анализа сетевой нагрузки определяет контрольные характеристики, в качестве которых были выбраны: скорость потока данных, скорость увеличения скорости потока данных, задержка, скорость изменения задержки, энтропия, параметр Херста, Пуассоновский поток данных.

До момента начала DDoS-атаки система анализа сетевой нагрузки строит контрольные характеристики для нормальной структуры трафика, на основании которых впоследствии определяются аномалии при атаке.

Система анализа сетевой нагрузки состоит из модулей анализа трафика, сканирования портов и мониторинга сетевой нагрузки.

Модули анализа трафика перехватывают в режиме реального времени сетевой трафик, направленный на сервер. Во время работы сетевой интерфейс переключается в «режим прослушивания» (Promiscuous mode), что и позволяет ему получать пакеты, адресованные другим интерфейсам в сети. Модуль «Анализатор трафика» сканирует компьютер на наличие сетевых адаптеров с пометкой работающих и неработающих, перехватывает в режиме реального времени пакеты TCP и IP с указанием IP-адреса получателя и IP-адреса отправителя, времени перехвата, длины пакетов, портов отправителя и получателя, а также измеряет задержку ответов узла на запросы.

Модуль «Сканирование портов» сканирует порты TCP и UDP с указанием локальных адресов, локальных портов, внешних адресов, внешних портов, определяет информацию о состоянии активности портов, ID и имени процесса. Данный модуль реализован с помощью утилиты командной строки операционной системы Windows netstat (network statistics) и технологий, которые использовались при создании программы Zenmap.

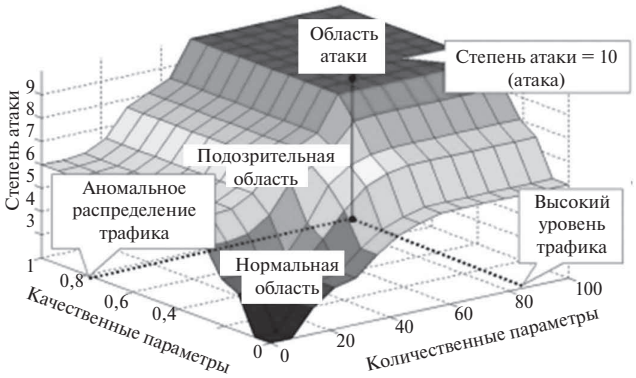

Рисунок 1. Работа механизмов поведенческого анализа

Модуль «Мониторинг сетевой нагрузки» обрабатывает статистические данные, полученные в результате сканирования сети анализатором трафика, методом определения состояния DDoS-атаки по статистическим параметрам сетевого трафика. После обработки данные отображаются в виде следующих графиков: скорости потока данных (скорость трафика), скорости увеличения скорости потока данных, Пуассоновского распределения данных, энтропии, параметра Херста, задержки, скорости изменения задержки. Модуль «Мониторинг сетевой нагрузки» обладает расширенными графическими инструментами для более удобного анализа графиков, включая возможности отображать графики как по одиночке, так и группами, автоматического масштабирования графиков, изменения цветового фона на более удобный, распечатки графиков.

Для полноценной оценки работоспособности системы анализа сетевой нагрузки было проведено полнофункциональное тестирование.

Для проведения анализа сетевой нагрузки в главном окне приложения нужно нажать на кнопку «Сканировать устройства для прослушивания сети», после чего в списке появятся сетевые адаптеры, которые были обнаружены на компьютере или сервере. Запуск процесса перехвата сетевых пакетов производится нажатием на кнопку «Старт» (рис. 2). На данный момент приложение не имеет

Рисунок 2. Интерфейс главного окна системы

возможности строить графики по всем характеристикам в реальном времени, поэтому для отображения графической информации необходимо остановить процесс перехвата (кнопка «Финиш») (рис. 2). Приложение остановит процесс перехвата сетевых пакетов и сообщит об этом пользователю.

После нажатия на кнопку «Анализ» (рис. 2) по завершении процесса перехвата сетевых пакетов открывается новое окно программы, в котором представлены графики. По этим графикам можно с большой точностью определить начало DDoS-атаки. Графики могут выводиться на экран как по одному, так и группой, для более удобного восприятия информации.

Для более глубокого анализа предусмотрена функция распечатки графиков.

Тестирование при обычной и резко возрастающей нагрузке

Скорости потока данных при обычной и возрастающей нагрузках отличаются количеством пакетов в секунду. Скорость потока данных при обычной нагрузке на графике в среднем приблизительно равно 10 пакетам в секунду, а сам график в среднем, несмотря на наличие шума, будет представлять собой горизонтальную линию (рис. 3). Скорость потока данных при возрастающей нагрузке на графике постоянно увеличивается и в пике достигает почти 1500 пакетов в секунду, а сам график будет в среднем возрастающей линией (рис. 4).

Скорость увеличения скорости потока данных при обычной нагрузке на графике в среднем – плавно

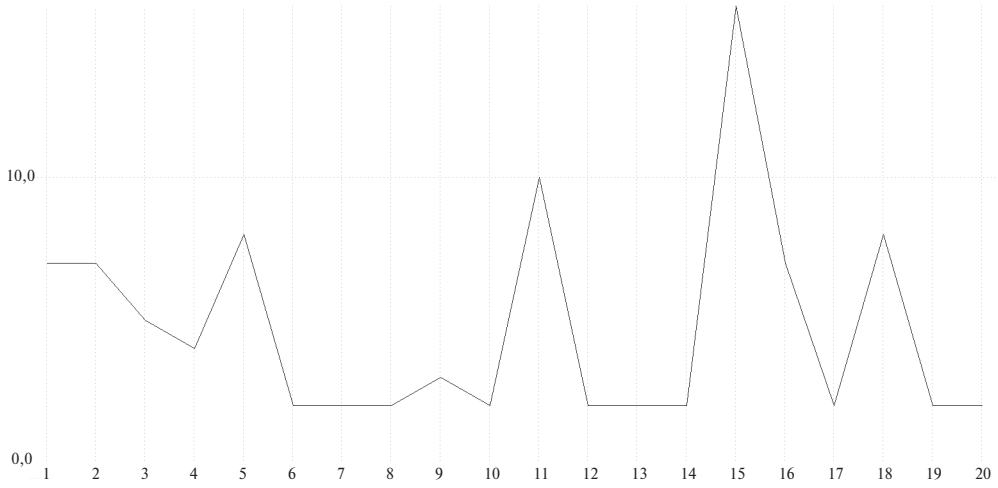

Рисунок 3. Скорость потока данных при обычной нагрузке

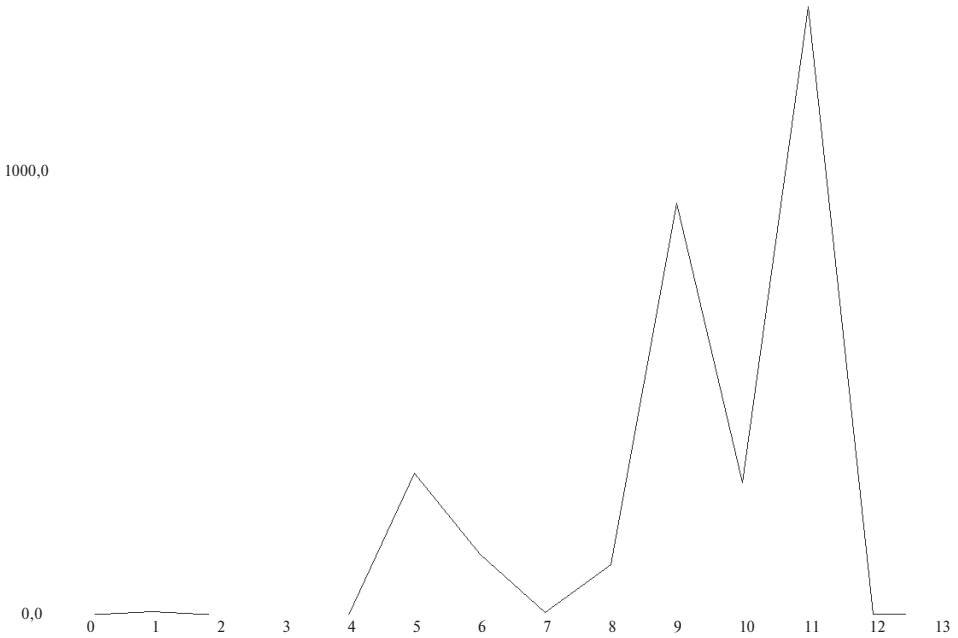

Рисунок 4. Скорость потока данных при резко возрастающей нагрузке

убывающая линия (рис. 5), а при возрастающей нагрузке может представлять собой или прямую, или возрастающую линию (рис. 6).

Пуассоновский поток данных при обычной нагрузке на графике – симметричная парабола, которая стремится к горизонтальной линии (рис. 7). Пуассоновский поток данных при возрастающей нагрузке на графике представляет собой резко выраженную несимметричную параболу (рис. 8).

В данной статье приведена только часть результатов проведенных экспериментов. Разработанная система мониторинга позволяет отслеживать семь различных статистических параметров трафика, что способствует более точному выявлению

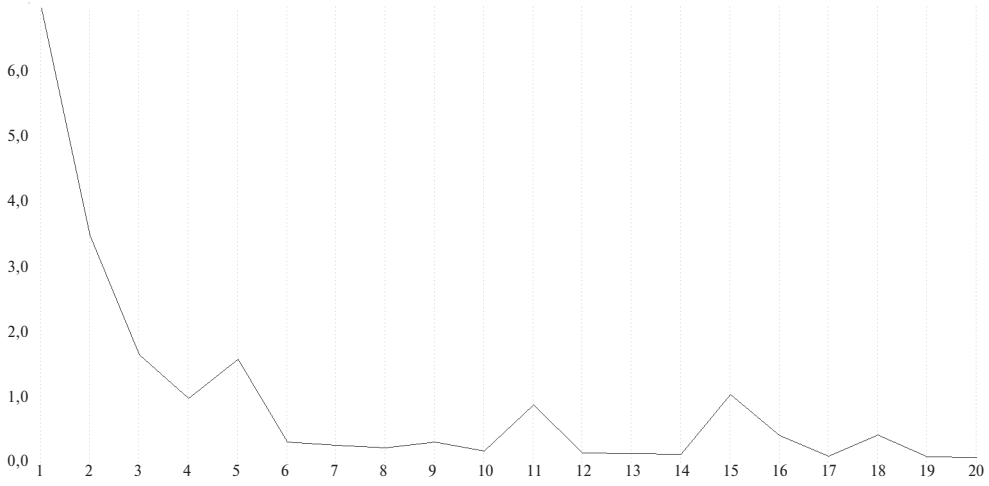

Рисунок 5. Скорость увеличения скорости потока данных при обычной нагрузке

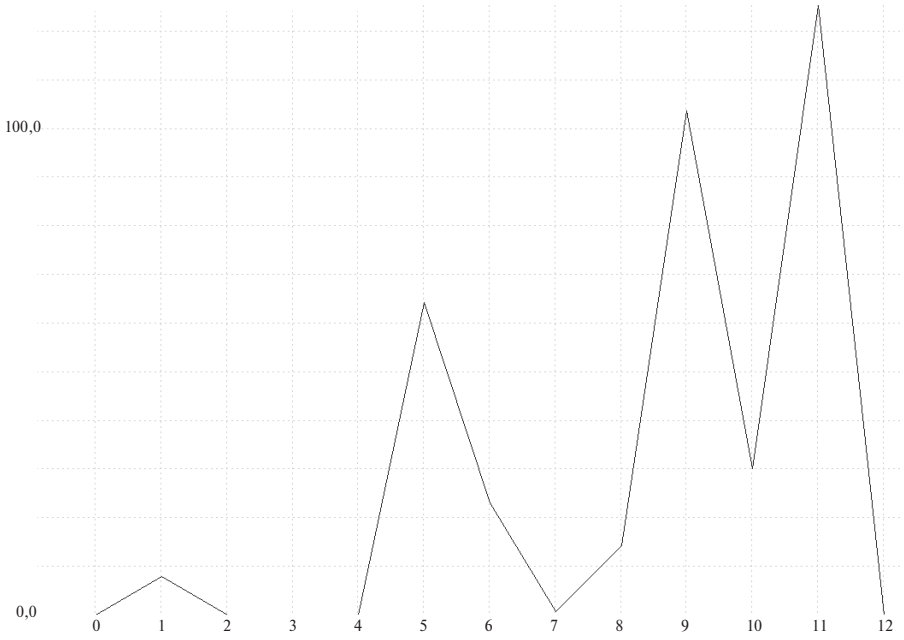

Рисунок 6. Скорость увеличения скорости потока данных при возрастающей нагрузке

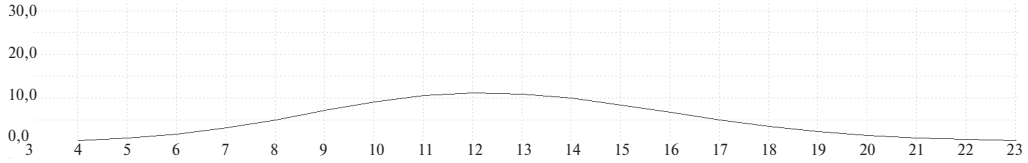

Рисунок 7. Пуассоновский поток данных при обычной нагрузке

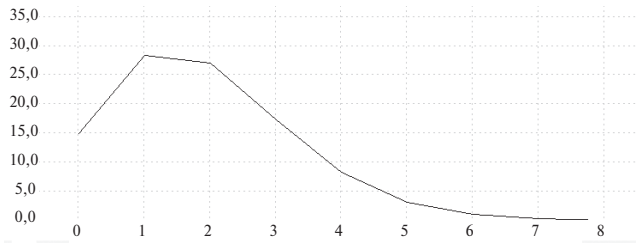

Рисунок 8. Пуассоновский поток данных при возрастающей нагрузке

аномалий, свидетельствующих о начале DDoS-атаки. Также система снабжена дополнительным инструментарием для удобства работы с сетью, что позволяет с уверенностью говорить о возможности ее применения для реальных задач на серверах или критичных узлах сети.

Выводы

Разработанный программный продукт дает возможность отследить даже незначительные аномалии в трафике, что позволяет на практике определить факт начала DDoS-атаки с высокой степенью точности. Так как применяется анализ большого числа статистических параметров, можно говорить о возможности выявления любого вида подобного рода атак на любом уровне модели OSI (open systems interconnection basic reference model – базовая эталонная модель взаимодействия открытых систем). Система может применяться для выявления факта начала атаки на отказ в обслуживании на серверах и маршрутизаторах локальных и глобальных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Халимоненко А., Купреев О., Бадовская Е. DDoS-атаки в первом квартале 2018 года. [Электронный ресурс]. URL: https://securelist.ru/ddos-report-in-q1–2018/89700/ (дата обращения: 29.07.2018).
2. DDoS-атаки и методы борьбы с ними. [Электронный ресурс]. URL: http://www.internet-technologies.ru/articles/ddos-ataki-i-metody-borby-s-nimi.html (дата обращения: 29.07.2018).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Жарова Ольга Юрьевна, старший преподаватель, Калужский филиал ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (Национальный исследовательский университет)», Российская Федерация, 248000, Калуга, ул. Баженова, д.2, тел.: 8 (4842) 22-48-84, e-mail: ouzharova@yandex.ru.

For citation: Zharova O.Yu. Application of network load analysis system for detecting start of DDoS attack. Voprosy radioelektroniki, 2018, no. 11, pp. 48–52.
DOI 10.21778/2218-5453-2018-11-48-52

O.Yu. Zharova

APPLICATION OF NETWORK LOAD ANALYSIS SYSTEM FOR DETECTING START OF DDOS ATTACK

Different web resources including state and geoinformational systems can be exposed to denial of service (DDoS) attacks. The goal of this investigation is determining the efficiency of developed system for network load analysis. Problem of DDoS-attacks is considered together with existing methods and measures for counteraction of such kinds of attacks. An approach to determining attack beginning is examined in details. Developed system, its architecture and functionality of each module are described. Testing results are given for both normal traffic conditions and abruptly increasing load, which models avalanche DDoS-attack. The system builds graphs to visualize monitoring process which definitely show attack beginning. A conclusion is made that the system can be used for DDoS-attack detection.

Keywords: distributed denial of service, statistical parameters, traffic

REFERENCES

1. Khalimonenko A., Kupreev O., Badovskaya E. DDoS attacks in the first quarter of 2018. (In Russian). Available at: https://securelist.ru/ddos-report-in-q1–2018/89700/ (accessed 29.08.2018).
2. DDoS attacks and methods of dealing with them. (In Russian). Available at: http://www.internet-technologies.ru/articles/ddos-ataki-i-metody-borby-s-nimi.html (accessed 29.08.2018).

AUTHOR

Zharova Olga, senior teacher, Bauman Moscow State Technical University (Kaluga Branch), 2, Bazhenova St., Kaluga, 248000, Russian Federation, tel.: +7 (4842) 22-48-84, e-mail: ouzharova@yandex.ru.