УДК 004.056
DOI: 10.15827/0236-235X.133.083-090
Дата подачи статьи: 28.12.20
2021. Т. 34. № 1. С. 083–090

Использование энтропийных характеристик сетевого трафика для определения его аномальности

А.Ю. Ефимов [1], *заведующий отделом, efimovay@cps.tver.ru*

[1] *НИИ «Центрпрограммсистем», г. Тверь, 170024, Россия*

Количество и масштабы сетевых компьютерных атак (вторжений) постоянно растут, что делает высокоактуальной задачу их оперативного обнаружения. Для этого применяются системы обнаружения вторжений уровня сети, опирающиеся на два подхода – обнаружение злоупотреблений и обнаружение аномалий, причем второй подход видится более перспективным в условиях постоянного появления новых и модифицированных видов вторжений. Основными объектами применения техник обнаружения аномалий являются атаки массового характера (DoS- и DDoS-атаки, сканирования, распространение вирусов-червей и т.п.), которые трудно обнаружить другими (например, сигнатурными) методами, так как в их основе часто лежат штатные сетевые взаимодействия.

Метод анализа энтропии для обнаружения аномалий сетевого трафика по сравнению со многими другими методами характеризуется достаточно простой реализацией и скоростью работы. Применение метода основано на общем предположении, что аномальный трафик более упорядочен или структурирован, чем обычный трафик, в одних параметрах и более хаотичен в других, что проявляется в виде снижения или роста энтропии этих параметров.

Данная статья посвящена определению характера влияния атак на энтропию таких параметров трафика, как IP-адреса источника и назначения, а также порт назначения, рассматривая в качестве объектов DoS- и DDoS-атаки нескольких разновидностей. Описывается подход к определению энтропии (с использованием энтропии Шеннона). Приведены результаты проведенного автором моделирования, наглядно демонстрирующие неоднозначность влияния атак на энтропийные характеристики. Показана явная зависимость характера влияния (снижение или рост) от таких факторов, как источник, цель, мощность атаки, а также распределение нормального трафика.

Сделаны выводы о возможности эффективного обнаружения аномалий, соответствующих DoS- и DDoS-атакам, путем анализа энтропии параметров сетевого трафика, но только при условии проведения данного анализа с учетом распределения нормального трафика и объемных характеристик нормального и суммарного трафиков.

Ключевые слова: *обнаружение вторжений, компьютерная атака, обнаружение аномалий, анализ энтропии, сетевой трафик, атака отказа в обслуживании, распределенная атака отказа в обслуживании.*

Внедрение компьютерных информационных технологий практически во все сферы деятельности человека уже давно является объективной тенденцией. При этом сложность таких технологий постоянно растет, увеличиваются номенклатура и объем обрабатываемых данных. Как следствие, увеличиваются сложность и масштабы локальных и корпоративных сетей, осуществляющих обработку информации, усложняется структура информационных потоков. Применение подобных технологий в задачах, существенных с точки зрения безопасности (обработка сведений различной степени конфиденциальности, управление технологическими процессами и т.п.) в условиях постоянного роста осуществляемых сетевых компьютерных атак [1, 2], очевидно, должно сопровождаться соответствующими мерами и средствами по обеспечению защиты как обрабатываемой информации, так и систем, осуществляющих эту обработку.

Подходы к обнаружению вторжений

Одним из эффективных подходов к обеспечению защиты от сетевых компьютерных атак (вторжений) различного рода является применение *систем обнаружения вторжений* (СОВ) уровня сети. Данные системы позволяют выявлять вторжения путем анализа сетевого трафика с помощью различного рода методов и алгоритмов. Одной из систем, обеспечивающих обнаружение вторжений на уровнях узла и сети с использованием как сигнатурных, так и эвристических методов, является программный комплекс обнаружения вторжений «Ребус-СОВ» (ПК «Ребус-СОВ») [3], разработанный НИИ «Центрпрограммсистем», что подтвер-

ждается сертификатом Федеральной службы по техническому и экспортному контролю Российской Федерации на соответствие документам «Методический документ. Профиль защиты систем обнаружения вторжений уровня сети второго класса защиты» ИТ.СОВ.С2.ПЗ и «Методический документ. Профиль защиты систем обнаружения вторжений уровня узла второго класса защиты» ИТ.СОВ.У2.ПЗ.

В СОВ используются два основных подхода к обнаружению вторжений – обнаружение злоупотреблений и обнаружение аномалий [4, 5].

Обнаружение злоупотреблений основано на определении соответствия контролируемых параметров трафика некоторому заранее сформированному набору шаблонов (сигнатур) известных типов вторжений. Очевидно, что в статике методы обнаружения злоупотреблений неэффективны как для новых видов вторжений, так и для модификаций ранее известных. Адаптация к их появлению осуществляется путем регулярного дополнения баз сигнатур вторжений и их актуализации на месте применения, что заведомо является длительным процессом.

Обнаружение аномалий предусматривает создание некоторых профилей штатной деятельности контролируемого объекта (на уровне сети, ЭВМ, пользователя и т.п.). Выявление вторжений при этом основано на определении степени отклонения текущего поведения объекта от сформированного профиля [6]. Для решения задач формирования профилей и выявления отклонений от них используется целый ряд различных методов, таких как методы машинного обучения, методы вычислительного интеллекта, поведенческие методы [7, 8].

Аномалии сетевого трафика

Основным применением техник обнаружения аномалий при обнаружении вторжений является обнаружение таких явлений, как DoS- и DDoS-атаки, сканирование сетей и портов, деятельность вирусов-червей и т.п. Сложность их выявления другими методами (например, сигнатурным) заключается в том, что в основе их часто лежат совершенно штатные сетевые взаимодействия, которые лишь по совокупности своего применения составляют угрозу для объекта (объектов) атаки. Например, обычный запрос html-страницы у веб-сервера является штатной и допустимой операцией. В то же время несколько тысяч или миллионов таких запросов, направленных на один сервер за короткий интервал времени, вполне могут нарушить доступность сервера, реализуя DoS- или DDoS-атаку. При этом необходимо учитывать, что схожий эффект может дать и всплеск легальной активности (так называемые флэш-события), когда, например, на сервере появился высоковостребованный контент и множество пользователей пытаются его получить. Аналогичная логика применима и к сканированию сетей и портов, которое, хотя и не наносит ущерба объекту сканирования, но зачастую является либо подготовительной стадией для целевой атаки (например, с использованием выявленной уязвимости), либо признаком деятельности зловредного ПО – червей и т.п.; это очевидно указывает на высокую потребность оперативного выявления подобного рода действий для предотвращения или хотя бы минимизации последствий атак.

Выявление подобного рода активности на уровнях отдельных сетевых пакетов и сессий (на которых чаще всего применяется сигнатурный анализ) в общем случае по указанным выше причинам нереализуемо. Для этого необходим анализ на уровне суммарного трафика, основанный на использовании методов статистики и теории информации.

Анализ энтропии для обнаружения аномалий сетевого трафика

Анализ энтропии является одной из разновидностей поведенческих методов обнаружения аномалий, которой (в отличие от многих других разновидностей, таких как вейвлет-анализ и спектральный анализ) не свойственны в большой степени такие недостатки, как сложность реализации и затраты времени [8], что в условиях постоянного роста объема сетевого трафика и скорости его передачи является существенным достоинством. Анализ энтропии применяется для формирования статистического критерия, с помощью которого возможно определение принадлежности рассматриваемого экземпляра сетевого трафика (а точнее, его параметров) к аномальному классу.

В основном применение данного метода к выявлению аномалий сетевого трафика основано на предположении, что аномальный трафик более упорядочен или структурирован, чем обычный трафик, в одних параметрах (что отражается снижением их энтропии) и более хаотичен в других (что отражается ростом их энтропии).

Конкретные применения данного метода достаточно разнообразны. Например, в [9] с це-

лью выявления DoS/DDoS-атак в локальной сети контролируемый сетевой трафик делится по временным окнам фиксированной длительности, для каждого окна оцениваются характеристики трафика (энтропия длительности сессии, уникальных IP-адресов источника, количества соединений с сервером, а также среднее время сессии), после чего производятся сопоставление данных характеристик с эталоном и выдача заключения о наличии или отсутствии аномалии (то есть атаки). Построение и использование соответствующих моделей разных видов атак позволяют дополнительно определять вид выявленной атаки.

Другой подход, ориентированный на выявление DDoS-атак, описан в [10]. Он предполагает разделение трафика в пределах временного окна на уникальные сетевые потоки и расчет энтропии множества этих потоков по IP-адресу источника. Далее на основании оценки информационного расхождения текущей метрики и нормальной, а также количества пакетов потоков выполняется классификация трафика на нормальный, DDoS-атаку (высокой или низкой интенсивности) или флэш-событие (всплеск легитимного трафика).

Описанный в [11] подход, в свою очередь, ориентирован на выявление атак типа «сканирование», для чего оценивается энтропия количества пакетов для сетевых взаимодействий (сетевых потоков) за фиксированный промежуток времени или для фиксированного количества сетевых пакетов. Подход основан на предположении, что наличие сканирующих пакетов в трафике увеличивает такую энтропию, что позволяет повысить обоснованность заключения о выявлении атаки типа «сканирование».

Применение анализа энтропии для выявления сетевой активности различных вирусов описано в [12], где предлагается оценивать изменения энтропии IP-адресов источника и назначения, а также энтропии сетевых портов, собирая данные с использованием метода скользящего окна с фиксированной периодичностью. При этом рассчитывается не собственно значение энтропии, а степень сжатия потоков контролируемых характеристик. На примерах действий отдельных вирусов показан принцип их возможного детектирования.

Характер влияния DoS- и DDoS-атак на энтропийные характеристики трафика

Рассмотрение описанных выше работ в целом показало наличие влияния аномального трафика на энтропийные характеристики суммарного трафика. Однако конкретный характер такого влияния на энтропию конкретных параметров трафика описан либо общими словами, либо для достаточно частных случаев. В связи с этим далее проанализируем характер влияния различных видов вторжений (на примерах нескольких разновидностей DoS- и DDoS-атак), рассматривая такие базовые параметры IP-трафика, как IP-адреса источника и назначения, а также сетевые порты назначения. Параметр порта источника в данном случае исключаем из рассмотрения, так как используемые при атаках порты зависят от конкретной реализации атакующего средства, а также от структуры сети на маршруте от источника до объекта атаки; порты могут быть и одинаковыми (что приведет к снижению энтропии данного показателя), и разными (что в зависимости от масштаба атаки может привести к росту энтропии, а может и не привести). Таким образом, рассмотрение данного параметра в общем случае не имеет смысла, хотя и может применяться для классификации конкретных атакующих средств.

В ходе исследования для расчета энтропии множества X будем использовать формулу Шеннона:

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x),$$

где $P(x)$ – вероятность появления элемента x в множестве X.

DoS-атака на сервис представляет собой большое количество обращений к конкретному сервису на узле-сервере с одного узла-источника. Соответственно, в общем трафике будет большое количество пакетов с одинаковыми IP-адресом источника (источник атаки), IP-адресом назначения (атакуемый сервер) и портом назначения (атакуемый сервис). Интуитивно можно предположить, что такая атака за счет концентрации трафика на общем узле-источнике и общем узле и порту назначения характеризуется снижением энтропии IP-адресов источника и назначения, а также порта назначения. Проведенное моделирование показало, что в целом такое предположение верно, однако имеется ряд нюансов, которые нужно учитывать при практическом использовании.

Рассмотрим влияние DoS-атаки на энтропию IP-адресов источника. Для моделирования нормального трафика используем произвольное распределение трафика, попадающего в временное окно фиксированной длительности, по IP-адресам источника, применяя в качестве

вероятностей отношение количества пакетов с нужным адресом к общему количеству пакетов во временном окне. Для моделирования атаки будем дополнять исходное распределение атакующим трафиком как для адресов, входящих в нормальный трафик, так и для новых адресов. Мощность атаки (условный количественный показатель, отражающий количество элементов атаки – пакетов, соединений и т.п., приходящихся на рассматриваемое временное окно) при моделировании варьируется для определения характера ее влияния на энтропию. Показательные результаты моделирования отражены на рисунке 1.

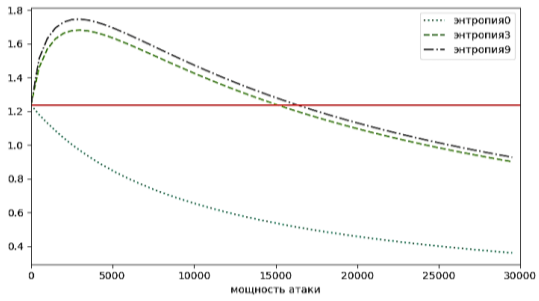

Рис. 1. Влияние параметров DoS-атаки на энтропию IP-адресов источника

Fig. 1. Impact of DoS attack parameters on entropy of source IP addresses

На рисунке горизонтальная линия соответствует энтропии нормального трафика (при отсутствии атаки), графики «энтропияX» показывают энтропию при атаках различной мощности и с различных адресов. При этом график «энтропия0» соответствует атаке с IP-адреса с максимальным нормальным трафиком, «энтропия3» – атаке с IP-адреса с небольшим нормальным трафиком, «энтропия9» – атаке с IP-адреса, не генерирующего нормальный трафик. Как видно из рисунка, чистое снижение энтропии при атаке наблюдается только в случае атаки с наиболее активного в нормальном режиме узла (что является редким случаем). При атаке же с любого другого узла, как генерирующего, так и не генерирующего нормальный трафик, сначала наблюдается рост энтропии по сравнению со значением для нормального трафика, и лишь при превышении мощностью атаки некоторого значения, зависящего от распределения нормального трафика, энтропия для трафика с атакой становится меньше значения для нормального трафика.

За счет адресной симметричности DoS-атаки на сервис (один узел-источник и один узел-цель) характер влияния такой атаки на энтропию IP-адресов назначения идентичен таковому для IP-адресов источника. Кроме того, за счет нацеленности такой атаки на конкретный порт назначения характер ее влияния на энтропию порта назначения также аналогичен.

Из полученных результатов моделирования можно сделать вывод, что энтропии IP-адресов источника и назначения, а также порта назначения из-за их зависимости от источника, цели и мощности атаки, а также от параметров нормального трафика самостоятельно могут использоваться для детектирования и классификации DoS-атак на сервис только при мощности атаки, значительно превышающей суммарный нормальный трафик. Для их применения в общем случае обязателен дополнительный учет параметров нормального трафика.

DoS-атака на сервер отличается от DoS-атаки на сервис направленностью на узел-сервер в целом. Этот факт отменяет детерминированность влияния такой атаки на энтропию порта назначения (так как используемые при атаке порты назначения будут зависеть от реализации атакующих средств и заранее неизвестны) и позволяет распространить на нее описанные для атаки на сервис результаты по влиянию на энтропии IP-адресов.

DoS-атака на сеть отличается от DoS-атаки на сервер тем, что в качестве узла назначения в ней участвуют разные узлы атакуемой сети (в том числе возможно появление реально не используемых в сети адресов). В связи с этим результаты влияния DoS-атаки сети на энтропии IP-адреса источника аналогичны таковым для описанных выше разновидностей DoS-атак, а влияние на энтропию IP-адресов назначения, очевидно, отличается. Определим характер этих различий с помощью моделирования. Для моделирования нормального трафика используем произвольное распределение трафика, попадающего в временное окно фиксированной длительности, по IP-адресам назначения. Для моделирования атаки дополним исходное распределение атакующим трафиком в следующих вариантах:

– сосредоточенная атака на небольшое количество реальных узлов сети (включая наиболее активные);

– сосредоточенная атака на небольшое количество реальных узлов сети (исключая наиболее активные);

– сосредоточенная атака на небольшое количество нереальных узлов сети;

– рассеянная атака на большое количество узлов сети (реальных и нереальных).

Мощность атаки при моделировании варьируется для определения характера ее влияния на энтропию.

Результаты моделирования для первых трех вариантов представлены в разных масштабах на рисунке 2 (графики «энтропия0», «энтропия5» и «энтропия7» соответственно). Результаты моделирования для последнего варианта представлены на рисунке 3 («энтропия256»). Горизонтальная линия на рисунках 2 и 3 соответствует энтропии нормального трафика (при отсутствии атаки). При моделировании всех вариантов использовалось одно и то же распределение нормального трафика.

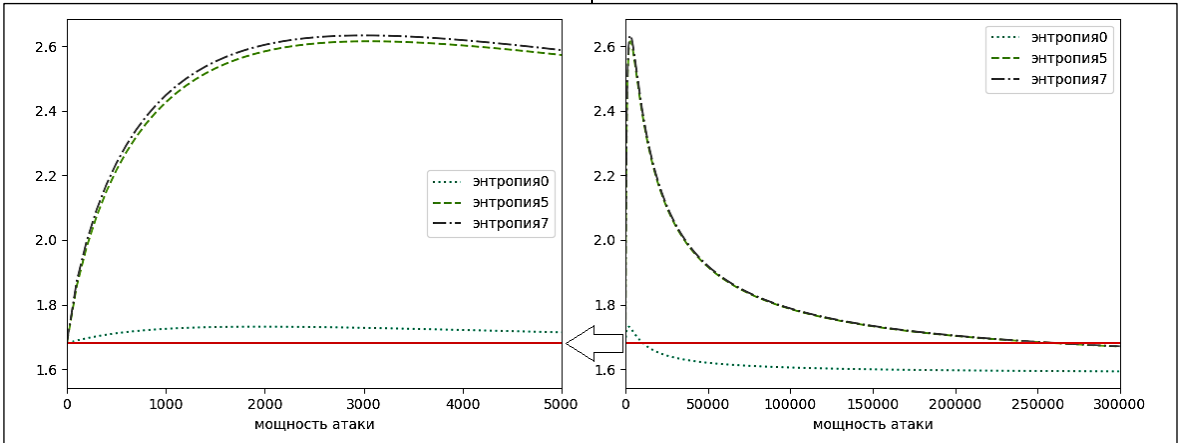

Рис. 2. Влияние параметров сосредоточенной DoS-атаки сети на энтропию IP-адресов назначения

Fig. 2. Impact of concentrated network DoS attack parameters on entropy of destination IP addresses

Как видно из рисунка 2, распространение атаки на несколько узлов сети (небольшое их количество относительно размеров сети) приводит к исключению варианта постоянно снижающейся энтропии, характерного для DoS-атаки на сервис или сервер, принимающий максимальный нормальный трафик. Как следствие, при относительно небольших мощностях атаки энтропия IP-адресов назначения возрастает (становится больше значения для нормального трафика), и лишь при превышении мощностью атаки некоторого порога, определяемого распределением нормального трафика, указанная энтропия становится меньше значения без атаки. При этом и амплитуда изменения энтропии, и пороговое значение мощности атаки могут существенно (на порядки) отличаться для разных распределений нормального трафика.

В случае, когда атака на сеть осуществляется полномасштабно, с использованием всех адресов сети (включая реально не используемые) или большей их части, характер ее влияния на энтропию IP-адресов назначения кардинально меняется, что хорошо видно на рисунке 3. Равномерное (или близкое к нему) распределение целевых адресов даже при достаточно небольших мощностях атаки легко перекрывает исходное распределение нормального трафика и приводит к существенному росту энтропии. Причем, в отличие от сосредоточенной атаки, даже при особо высоких мощностях рассеянной атаки снижения энтропии не происходит, что объясняется стремлением итогового распределения целевых адресов к нормальному с ростом мощности атаки и, как следствие, стремлением энтропии к ее предельному значению, определяемому выражением $\log_2 N$, где N – мощность множества IP-адресов сети.

Из полученных результатов моделирования атак на сеть можно сделать вывод, что энтропии IP-адресов назначения из-за их зависимости от мощности атаки, а также от параметров нормального трафика самостоятельно могут использоваться для детектирования и классификации только сильно рассеянных DoS-атак на сеть. Для применения таких энтропий в общем случае, как и для DoS-атак на сервис или на сервер, обязателен дополнительный учет параметров нормального трафика.

DDoS-атака отличается от DoS-атаки множественностью узлов-источников атаки. Как следствие, ее влияние на энтропию параметров трафика идентично таковым для DoS-атаки, за исключением энтропии IP-адреса источника. Применительно к данному параметру легко просматривается его схожесть с энтропией IP-адреса назначения при DoS-атаке на сеть (как сосредоточенной – для случая DDoS-атаки с небольшого количества внешних узлов, так

Рис. 3. Влияние параметров рассеянной DoS-атаки сети на энтропию IP-адресов назначения

Fig. 3. Impact of dispersed network DoS attack parameters on entropy of destination IP addresses

и рассеянной – для случая DDoS-атаки с большого количества узлов). Следствием данной схожести, подтверждаемой результатами моделирования, является возможность применения выводов по энтропии IP-адресов назначения для DoS-атаки на сеть к энтропии IP-адресов источника для DDoS-атак.

Заключение

Проведенные анализ и моделирование подтвердили явное влияние DoS- и DDoS-атак на энтропию таких параметров сетевого трафика, как IP-адреса источника и назначения, а также сетевые порты назначения. Однако при этом была продемонстрирована неполная состоятельность базового для методов анализа энтропии предположения о том, что аномальный трафик более упорядочен или структурирован по сравнению с обычным трафиком в одних параметрах (что отражается снижением их энтропии) и более хаотичен в других (что отражается ростом их энтропии). Как выяснилось, характер влияния атаки (аномалии) на энтропию параметров трафика (ее рост или снижение) во многих случаях зависит от распределения нормального трафика и мощности атаки, а также от ряда других факторов. Таким образом, энтропии указанных параметров сетевого трафика могут использоваться для эффективного обнаружения аномалий, соответствующих DoS- и DDoS-атакам, при условии, что их анализ осуществляется с учетом распределения нормального трафика, а также объемных характеристик нормального и суммарного трафиков.

Дальнейшее развитие данного исследования будет посвящено следующим направлениям:

− распространение описанного подхода на атаки других видов (в частности, сканирование портов, узлов, сети, распространение вирусов-червей и т.п.);

− сравнение качественных результатов и эффективности использованной в данном подходе энтропии Шеннона с другими видами энтропии (Цаллиса, Реньи);

− определение конкретных показателей нормального и суммарного трафиков, которыми необходимо дополнить анализ энтропии (для нивелирования неоднозначностей характера влияния атак на энтропии параметров трафика), а также методов их использования;

− определение эффективных методов для принятия решений по детектированию и классификации различных видов атак.

Реализацией результатов данного исследования планируется дополнить существующие методы статистического анализа сетевого трафика в ПК «Ребус-СОВ».

Литература

1. Актуальные киберугрозы: III квартал 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/ (дата обращения: 07.12.2020).

2. DDoS-атаки в III квартале 2020 года. URL: https://securelist.ru/ddos-attacks-in-q3-2020/99091/ (дата обращения: 07.12.2020).

3. Программный комплекс обнаружения вторжений «Ребус-СОВ». URL: https://rebus-sov.ru/ (дата обращения: 07.12.2020).

4. Лукацкий А.В. Обнаружение атак. СПб: БХВ-Петербург, 2003. 608 с.

5. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). М.: Горячая линия-Телеком, 2013. 220 с.

6. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999, vol. 31, no. 8, pp. 805–822. DOI: 10.1016/S1389-1286(98)00017-6.

7. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. 2016. Т. 2. С. 207–244. DOI: 10.15622/sp.45.13.

8. Добкач Л.Я. Анализ методов распознавания компьютерных атак // Правовая информатика. 2020. № 1. С. 67–75. DOI: 10.21681/1994-1404-2020-1-67-75.

9. Пенчев З.Н., Мансуров А.В. Метод идентификации сетевых атак с использованием эффективных характеристик статистических методов // Проблемы правовой и технической защиты информации. 2019. № 7. С. 30–38.

10. Behal S., Kumar K., Sachdeva M. A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics. TurkJElecEngCompSci, 2018, no. 26, pp. 1759–1770. DOI: 10.3906/elk-1706-340.

11. Гудков О.В. Характерные измеримые показатели атаки сетевого сканирования // Вестн. МГТУ им. Н.Э. Баумана. Сер.: Приборостроение. 2011. № S1. С. 60–66.

12. Морозов Д.И. Энтропийный метод анализа аномалий сетевого трафика в IP-сетях // Изв. ТРТУ. Технические науки. 2006. № 7. С. 120–124.

Software & Systems Received 28.12.20
DOI: 10.15827/0236-235X.133.083-090 2021, vol. 34, no. 1, pp. 083–090

Using the entropy characteristics of network traffic to determine its abnormality

A.Yu. Efimov [1], *Department Head, efimovay@cps.tver.ru*

[1] *R&D Institute Centerprogramsystem, Tver, 170024, Russian Federation*

Abstract. The number and scale of network computer attacks (intrusions) are constantly growing, which makes the problem of their prompt detection highly relevant. For this, network-level intrusion detection systems are used, based on two approaches – abuse detection and anomaly detection, and the second approach is more promising in the face of the constant appearance of new and modified types of intrusions. The main objects of application of anomaly detection techniques are mass attacks (DoS- and DDoS attacks, scanning, spreading of worm viruses, etc.), which are difficult to detect by other (for example, signature-based) methods, since they are often based on regular network interactions.

The entropy analysis method for detecting network traffic anomalies, compared to many other methods, is characterized by sufficient simplicity of implementation and speed of operation. The application of the method is based on the general assumption that abnormal traffic is more ordered or structured than normal traffic in some parameters and more chaotic in others, which manifests itself as a decrease or increase in the entropy of these parameters.

This paper is devoted to determining the nature of the impact of attacks on the entropy of such traffic parameters as the source and destination IP addresses, as well as the destination port, considering several types of DoS- and DDoS attacks as objects. The author describes an approach to determining entropy (using Shannon entropy). The paper presents the results of the author's model, which reveal the ambiguity of the impact of attacks on entropy characteristics. The results show a clear dependence of such inpact (decrease or increase) depends on factors such as the source, target, attack power, and distribution of normal traffic.

Conclusions are made about the possibility of effective detection of anomalies corresponding to DoS and DDoS attacks by analyzing the entropy of network traffic parameters, but only if this analysis is carried out taking into account the distribution of normal traffic and the volumetric characteristics of normal and total traffic.

Keywords: intrusion detection, computer attack, anomaly detection, entropy analysis, network traffic, denial of service attack, distributed denial of service attack.

References

1. *Actual Cyber Threats: Q3 2020*. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/ (accessed December 07, 2020) (in Russ.).

2. *DDoS attacks in Q3 2020*. Available at: https://securelist.ru/ddos-attacks-in-q3-2020/99091/ (accessed December 07, 2020) (in Russ.).

3. *Rebus-SOV Intrusion Detection Software Package.* Available at: https://rebus-sov.ru/ (accessed December 07, 2020) (in Russ.).

4. Lukatsky A.V. *Attack Detection*. St. Petersburg, 2003, 608 p. (in Russ.).

5. Shelukhin O.I., Sakalema D.Zh., Filinova A.S. *Intrusion Detection in Computer Networks (Network Anomalies)*. Moscow, 2013, 220 p. (in Russ.).

6. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems. *Computer Networks*, 1999, vol. 31, no. 8, pp. 805–822. DOI: 10.1016/S1389-1286(98)00017-6.

7. Branitskii A.A., Kotenko I.V. Analysis and classification of methods for network attack detection. *Proc. SPIIRAN*, 2016, vol. 2, pp. 207–244. DOI: 10.15622/sp.45.13 (in Russ.).

8. Dobkach L.Ya. An analysis of methods for identifying computer attacks. *Legal Informatics*, 2020, no. 1, pp. 67–75. DOI: 10.21681/1994-1404-2020-1-67-75 (in Russ.).

9. Penchev Z.N., Mansurov A.V. Method for identifying network attacks using effective characteristics of statistical methods. *Problems of Legal and Technical Protection of Information*, 2019, no. 7, pp. 30–38 (in Russ.).

10. Behal S., Kumar K., Sachdeva M. A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics. *TurkJElecEngCompSci*, 2018, no. 26, pp. 1759–1770. DOI: 10.3906/elk-1706-340.

11. Gudkov O.V. Typical measurable metrics of network scanning attack. *Herald of the Bauman Moscow State Technical University. Ser.: Instrument Engineering,* 2011, no. S1, pp. 60–66 (in Russ.).

12. Morozov D.I. Entropy method for analyzing network traffic anomalies in IP networks. *Izv. TRTU. Technical Sciences*, 2006, no. 7, pp. 120–124 (in Russ.).

Для цитирования

Ефимов А.Ю. Использование энтропийных характеристик сетевого трафика для определения его аномальности // Программные продукты и системы. 2021. Т. 34. № 1. С. 083–090. DOI: 10.15827/0236-235X.133.083-090.

For citation

Efimov A.Yu. Using the entropy characteristics of network traffic to determine its abnormality. *Software & Systems*, 2021, vol. 34, no. 1, pp. 083–090 (in Russ.). DOI: 10.15827/0236-235X.133.083-090.