Использование фрактальных мер для мониторинга состояния сети и вероятностного определения типа сетевой атаки

О.Ю. Губарева[1], О.В. Осипов[1], А.О. Почепцов[1], В.В. Пугин[1]
[1]ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Льва Толстого 23, Самара, Россия, 443010

Аннотация. В работе рассмотрен способ анализа сетевого трафика на предмет оценки рисков информационной безопасности сетевых узлов на основе фрактального анализа, учитывающий предысторию системы и позволяющий вероятностно оценить возможные типы сетевых атак на исследуемую систему. Предложена методика анализа сетевого трафика на основе совокупности фрактальных мер с целью анализа состояния сети и вероятностного определения типа атаки. На основе результатов работы планируется создание анализатора (сниффера) сетевого трафика для временной оценки состояния информационной безопасности, а также последующего вычисления ранее атакованных устройств и сетевых узлов.

1. Введение

Любая организация при осуществлении своей деятельности подвержена различным информационным рискам, которые, так или иначе, влияют, на специфику ведения бизнес-процессов и могут негативным образом повлиять как на финансовые показатели, так и на возможность организации продолжать бизнес. Современные требования бизнеса диктуют необходимость использования в своей работе обоснованных технико-экономических методов и средств, позволяющих количественно и качественно измерять уровень обеспечения информационной безопасности (ИБ), а также оценивать экономическую эффективность затрат на ИБ. Для эффективного обеспечения ИБ организаций, необходим серьезный, систематизированный и комплексный подход.

Следует отметить, что построение практически любой системы ИБ должно начинаться с анализа рисков. Прежде чем проектировать систему ИБ, необходимо определить, какие угрозы (то есть условия и факторы, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) существуют для данной информационной системы (ИС) и насколько они потенциально опасны.

Телекоммуникационные сети имеют множество уязвимостей, возникающих как при разработке системного программного обеспечения, так и при неправильной конфигурации и эксплуатации оборудования. Наличие угроз безопасности делает реальным возможность злоумышленникам реализовать различные виды сетевых атак. В настоящее время значительный интерес представляет разработка программных средств для анализа рисков ИБ путем оперативного анализа сетевого трафика. Определение возможных целей

предполагаемого нападения составляет основу проектирования системы обеспечения безопасности. Цели нападения показывают, что следует защищать. Как правило, анализируется состояние сети с целью решения задач сетевого администрирования, мониторинга маршрутизаторов и др. Для выявления аномального поведения системы чаще всего используется сбор и анализ различной статистической информации по IP-трафику. В данной работе для получения информации о сетевом трафике использовалось бесплатно распространяемое по лицензии GNU GPL программное обеспечение Zabbix. Система мониторинга при этом представляет совокупность программного обеспечения для снятия текущего трафика и программной системы его анализа, построенного на расчете значений, так называемых, фрактальных мер, которые будут в дальнейшем конкретизированы в предлагаемой работе.

2. Постановка задачи и метод решения

Целью работы является разработка методики анализа сетевого трафика на основе совокупности фрактальных мер с целью анализа состояния сети и вероятностного определения типа атаки. Основываясь на исследованиях, изложенных в данной работе, авторы планируют создать анализатор (снифер) сетевого трафика, оставшегося за последнее время на сервере компании, для его временной оценки, последующего вычисления ранее атакованных устройств и сетевых узлов (уязвимостей сети) и, как следствие, дальнейшей оценки рисков ИБ.

В работе [1] дан обзор научных исследований в области анализа сетевого трафика в режиме реального времени, а также рассмотрены конкретные программно-аппаратные решения.

В работе [2] рассматривается использование показателя Херста для анализа трафика, подверженного аномальным вторжениям в виде DoS-атак. Проведенные в [2] исследования показали, что трафик обладает свойством самоподобия во время аномальных вторжений, что доказывает возможность определения аномалий трафика в режиме реального времени.

Однако для более подробного анализа, кроме показателя Херста, весьма актуальным представляется исследование спектра мощности.

Для достижения поставленной цели в работе были решены следующие основополагающие задачи: проведение процессного анализа исследуемой ИС (за основу взята ИС образовательного учреждения) как объекта защиты; оценка показателя Херста, спектра мощности и фрактальных мер сетевого трафика в нормальном состоянии и в момент проведения атаки на ресурсы информационной системы; проведение атаки на ресурсы системы.

Фрактальный анализ по своей природе является статистическим и, кроме того, позволяет найти в исследуемом трафике признаки самоподобия. Этот факт позволяет, во-первых, выявить минимальное необходимое время проведения эксперимента, во-вторых, позволяет надеяться на возможность предсказания динамики поведения системы в ближайшем будущем. Фрактальная модель представляет собой совокупность фрактальных параметров (мер), поставленных в соответствие текущему состоянию сетевого трафика. Динамика изменения фрактальных мер при приведении ряда измерений состояния одного и того же телекоммуникационного узла позволяет судить о динамике состояния трафика, т.е. о наличии или отсутствии атак на ресурсы ИС. Забегая вперед, можно отметить, что в результате проведенного эксперимента было выявлено, что в случае DoS-атак снижается уровень самоподобия сетевого трафика, а также происходит преобразование спектра мощности.

Идея эксперимента состоит в следующем. Имеется телекоммуникационный трафик, а именно график зависимости нагрузки сети от времени (рисунок 1). С точки зрения математического анализа, исследуемый трафик представляет собой одномерный временной ряд, отсчеты которого представляют уровни загруженности канала в различные моменты

времени. Данный ряд может быть проанализирован при помощи расчета различных фрактальных мер (показатель Херста и др.), а также спектра мощности.

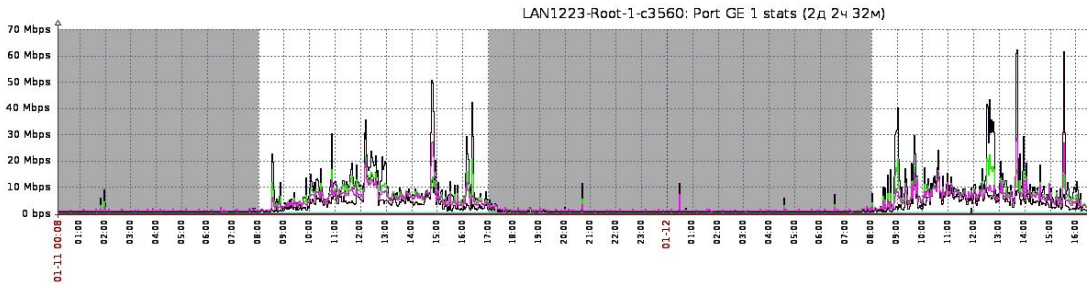

Рисунок 1. График зависимости зависимости нагрузки сети от времени

На первом этапе показатель Херста и спектр мощности были рассчитаны для нормального состояния сети.

Сначала вычисляется показатель Херста для определения уровня самоподобия сетевого трафика. Для его расчета находится среднее значение загруженности канала $\langle U \rangle_N$ за N временных отсчетов [3, 4]:

$$\langle U \rangle_N = \frac{1}{N} \sum_{n=1}^{N} U(n). \tag{1}$$

Далее вычисляется $X(n, N)$, представляющее собой накопившееся отклонение $U(n)$ от среднего значения $\langle U \rangle_N$, которое определяется следующей суммой:

$$X(n, N) = \sum_{p=1}^{n} \{U(p) - \langle U \rangle_N\}, \tag{2}$$

где среднее значение $\langle U \rangle_N$ определяется формулой (1).

Согласно методу нормированного размаха Херста [3, 4], размах отклонений определятся через минимальное и максимальное значения накопившегося отклонения $X(n, N)$ (2):

$$R(N) = \max_{1 \le n \le N} X(n, N) - \min_{1 \le n \le N} X(n, N). \tag{3}$$

Стандартное отклонение $S(N)$ можно вычислить по следующей известной формуле через дисперсию [3, 4]:

$$S(N) = \left\{ \frac{1}{N} \sum_{n=1}^{N} [U(n) - \langle U \rangle_N]^2 \right\}^{1/2}. \tag{4}$$

Для большинства временных рядов, наблюдаемый нормированный размах R/S описывается эмпирическим соотношением и с использованием (3) и (4) имеет вид [3, 4]:

$$R/S = (\alpha N)^H, \tag{5}$$

где H – показатель Херста; α – произвольная постоянная.

Описанная процедура в научной литературе получила название R/S-анализа.

На рис. 2 показана зависимость R/S телекоммуникационного трафика в нормальном состоянии от N в двойном логарифмическом масштабе. По оси ординат отложено значение $\lg(R/S)$, по оси ординат — $\lg N$. Значение показателя Херста для исследуемого

трафика в нормальном состоянии оказалось равным 0.68. Согласно теории фракталов, если полученное значение показателя Херста $H < 0.5$, исследуемый ряд обладает «кратковременной» памятью, то есть является антиперсистентным. Это означает, что недавние события в породившей его системе оказывают намного большее значение на дальнейшее поведение самой системы, чем события более ранние. Если $H > 0.5$, временной ряд персистентен и обладает фрактальной природой. При значении $H = 0.5$ сигнал представляет собой стохастический шум и не содержит полезной информации. Таким образом, было доказано, что исследуемый трафик в нормальном состоянии является самоподобным и обладает фрактальной природой.

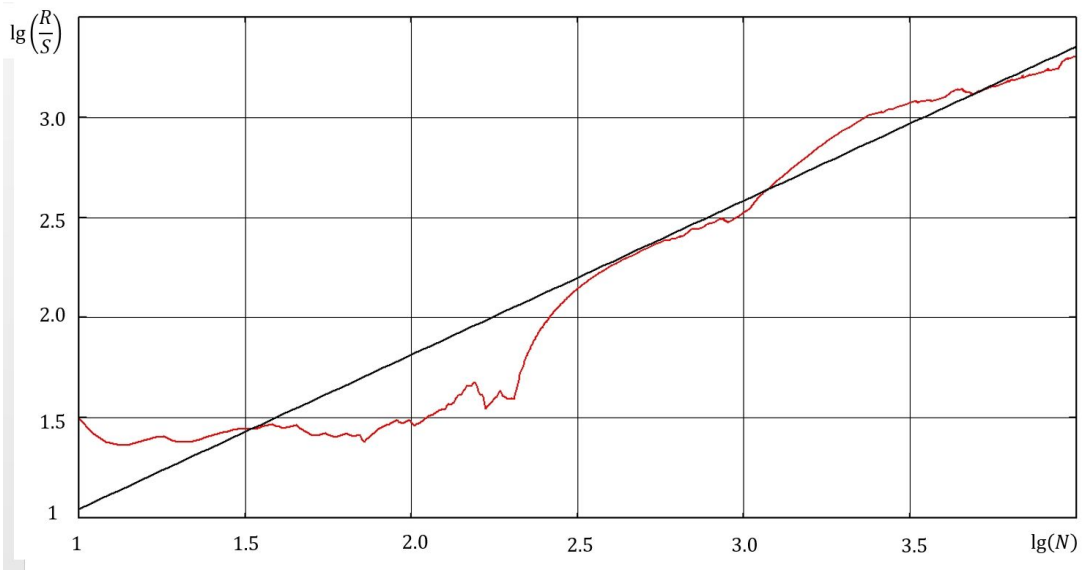

Рисунок 2. R/S зависимость телекоммуникационного трафика

Далее в работе проводилась оценка спектра мощности, который представляет собой быстрое преобразование Фурье автокорреляционной функции.

Автокорреляционная функция сетевого трафика определяется следующим выражением:

$$R(j) = \frac{1}{N} \sum_{i=1}^{N-j} U(i) U(i+j), \tag{6}$$

где N – общее количество временных отсчетов сетевого трафика.

Спектр мощности сигнала определяется прямым преобразованием Фурье автокорреляционной функции (6):

$$S_k = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{p=1}^{N-i} U(p) U(p+i) \exp\left[-j\frac{2\pi k i}{N}\right], \ \left(k = \overline{0, N-1}\right). \tag{7}$$

На рисунке 3 представлен спектр мощности $S(f) = S_k(U)$ сетевого трафика в нормальном состоянии (без наличия сетевой атаки).

На втором этапе исследовались фрактальные меры и спектр мощности сетевого трафика в состоянии DoS-атаки.

Во время DoS-атаки загрузка канала была полной и составляла 70 МБ/с. Здесь уместно заметить, что использование фрактальных мер (в частности, параметра R/S) позволяет

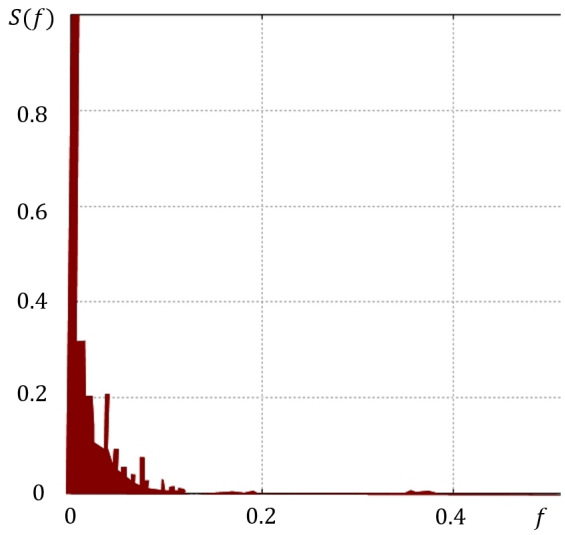

Рисунок 3. Спектр мощности сетевого трафика в нормальном состоянии

гарантировать масштабируемость полученных результатов и на случай более высокой загруженности канала.

Для проведения исследования была разработана заранее уязвимая web-система, имевшая заранее известный IP-адрес. Для DoS-атаки использовалось программное обеспечение, аналогичное программе LOIC, которое позволяет провести атаку по заранее заданному IP-адресу с изменяемым количеством запросов. Кроме того, одновременно с этим осуществлялась атака на MySQL-сервер путем внедрения SQL-инъекции через GET-параметр уязвимой системы.

Для этого использовался запрос с использованием SQL-функции benchmark (n, q), которая позволяет выполнять n раз функцию q [5].

Для атаки на SQL-сервер был использован скрипт, который в цикле заданное число раз отправлял подобные запросы. После выполнения DoS-атаки был снят сетевой трафик во время ее протекания, который был вновь проанализирован на значения фрактальных мер и спектра мощности. Значение показателя Херста для исследуемого трафика в состоянии атаки оказалось равным 0.54, что свидетельствует о резком уменьшении степени самоподобия исследуемого трафика.

В настоящее время проводятся эксперименты на магистральной сети с загрузкой 1,2 ГБ/с с длительностью временной выборки 24 часа (86000 расчетных значений загрузки канала).

На рисунке 4 показан спектр мощности для рассматриваемого случая, который по внешнему виду позволяет классифицировать исследуемый сигнал как «коричневый шум».

Таким образом, в результате эксперимента на реальной сети было доказано изменение фрактальных мер и спектра мощности сетевого трафика при наличии DoS-атаки.

Интерес представляет изучение фрактальных мер и спектра мощности сетевого трафика при наличии различных сетевых атак, что может привести к созданию некоторой интерактивной библиотеки «паттернов» спектров мощности и значений фрактальных мер, то есть речь идет о возможности создания некоторого фрактального индикатора состояния сети за некоторый интервал времени с повышенной вероятностью определения вида угрозы. Здесь уместно подчеркнуть, что тонкий фрактальный анализ

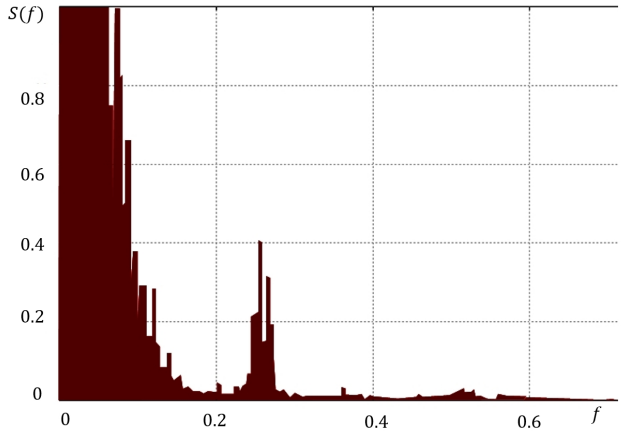

Рисунок 4. Спектр мощности сетевого трафика в момент проведения атаки

позволяет выявлять минимальные изменения трафика, несмотря на полную загруженность канала при наличии сетевой атаки. Но, впрочем, здесь необходимы дальнейшие экспериментальные исследования с целью выявления конкретных угроз и построения «паттернов» фрактальных характеристик. Заметим, что расчет показателя Херста сетевого трафика с 10000 временными выборками занимает около 1,5 секунд при использовании Intel Core i5, а расчет спектра мощности – около 4 секунд.

3. Заключение

Фрактальный индикатор состоянии сети должен выполнять следующие функции:

- сохранение выборки значений загруженности канала за определенные интервалы времени, достаточные для выявления состояния сети;
- расчет фрактальных мер и спектра мощности для каждого заданного временного ряда за определенный интервал с целью дальнейшего сравнения с «паттернами» из базы данных (использование нейронных сетей);
- вывод о состоянии сети в целом в текущий и предшествующие моменты времени;
- вероятностный прогноз о характере сетевой атаки в будущем.

Таким образом, в работе предлагается для анализа состоянии сетевого трафика (в том числе, при наличии DoS-атак) использовать фрактальные меры и спектр мощности, которые позволяют по косвенным признакам за приемлемый срок времени определять уровень угрозы. В заключение заметим, что предложенный метод лежит в основе создания фрактального индикатора для анализа состояния сети, при этом для определения источников DoS-атаки должны использоваться специализированные программные средства (iptables, ipwf и др.).

4. Литература

[1] Гетьман, А.И. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений / А.И. Гетьман, Ю.В. Маркин, Е.Ф. Евстропов, Обыденков Д.О. - Труды ИСП РАН. - 2017. - Т. 29(3). - С.117-150. DOI: 10.15514/ISPRAS-2017-29(3)-8.

[2] Шелухин, О.И. Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями / О.И. Шелухин, А.А. Антонян. – T-COMM: Телекоммуникации и транспорт. - 2014. - Т.8(6). - С. 61-64.

[3] Федер, Е. Фракталы / Е. Федер. - М: Мир, 1991. – 254 с.

[4] Головко, В.А. Нейросетевые методы обработки хаотических процессов / В.А. Головко // VII Всероссийская научно- техническая конференция «Нейроинформатика 2005». - М: МИФИ, 2005. - С.43-91.

[5] Низамутдинов, М.Ф. Тактика защиты и нападения на WEB-приложения / М.Ф. Низамутдинов - СПб.: БХВ-Петербург, 2005. – 432 с.

The using of fractal measures to network state monitoring and probabilistic network attack type determination

O.Yu. Gubareva[1], **O.V. Osipov**[1], **A.O. Pocheptsov**[1], **V.V. Pugin**[1]

[1]Povolzhskiy State University of Telecommunications and Informatics, Leo Tolstoy street 23, Samara, Russia, 443010

Abstract. The fractal analysis is used for the network traffic analysis of the information security of network nodes risks. The fractal analysis takes into account of the system history and allows probabilistic evaluation of possible network attacks types on the investigating system. A technique for analyzing network traffic based on a set of fractal measures was developed with the aim of analyzing the network state and probabilistic determination of the attack type. Based on the results of the work, it is possible to create an analyzer (sniffer) of network traffic for a temporary assessment of the information security state, as well as subsequent calculation of previously attacked devices and network nodes.

Keywords: information security, information system, risk, analysis, information, vulnerability, diagnostic system, stochastic model.