УДК 681.3

Р.Р. ФАТКИЕВА

МОДЕЛЬ ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ

Фаткиева Р.Р. **Модель обнаружения атак на основе анализа временных рядов.**
Аннотация. В статье рассматривается сравнительный анализ методов исследования входных и выходных данных и внутренних трафиков информационной системы. Предложен подход к обнаружению атак отказа в обслуживании, основывающийся на анализе временных рядов. Приводятся результаты обнаружения атак на основе пороговых значений.
Ключевые слова: сетевой трафик, атаки, временные ряды.

Fatkieva R.R. **Model of attack detection on the basis of time series analysis.**
Abstract. Comparativeanalysisofresearchmethodsofinformationsysteminput, output and inner traffic is carried out in the paper. The approach to denial-of-service attack detection on the basis of time series analysis is proposed. Results of attack detection by means of threshold value method are presented.
Keywords: network traffic, attack, time series.

1. Введение. Природа аномального поведения информационных систем (ИС) обусловлена чрезвычайной сложностью объекта, включающего огромное количество компьютерных устройств, систем передачи данных на основе системы взаимосвязанных протоколов и коллективной работы большого количества пользователей и системных администраторов. Поведение таких систем носит нелинейный характер [8]. Одним из доказательств нелинейности подобных систем является наличие системы прерывания в операционных системах [3]. С другой стороны, основные сетевые протоколы порождают хаотические структуры, выявленные при измерении сетевого трафика, и могут быть описаны на основе теории динамических систем (ДС) [8, 13]. Для большинства сетевых протоколов, применяемых в глобальных вычислительных сетях (в частности, стек протоколов TCP/IP), нелинейное поведение заложено в их алгоритмах (например, механизмы «медленного старта», борьба с перегрузками в вычислительных сетях) [8].

Динамические процессы в компьютерных сетях можно описать системой уравнений: $dx/dt = F(x,t)$, где x — вектор характеристик информационной системы; t — время. Трудным моментом моделирования является задание правой части. Определение вида функции $F(x,t)$ есть основная задача при исследовании ДС. В качестве одного из эффективных способов получения $F(x,t)$ применяется метод рекон-

струкции ДС по временным рядам [8,10,13], в нашем случае по сетевому трафику.

Традиционно начальным этапом является статистический анализ сетевого трафика. Из методов статистического анализа основное внимание уделяется проблемам сглаживания, трендам, автокорреляции, спектральному анализу, авторегрессии и др. Построение процедуры сглаживания на основе метода скользящего среднего [3] позволяет оценить тренд и построить упрощенную модель прогноза. Однако, необходимо помнить, что данная модель линейна и не может использоваться для критических условий. В работе [4] показано, что с помощью экспоненциального сглаживания с параметром сглаживания 0,21 возможно своевременное предупреждение о последующих выбросах сетевого трафика.

Наряду с методами экспоненциального сглаживания используется также аппроксимация полиномиальными трендами [4, 5], которая позволяет выделить детерминированную составляющую и оценить суточную и сезонную составляющие. Сезонная компонента трафика возникает за счет цикличности, присущей человеческой деятельности. Циклическая составляющая описывает нерегулярные подъемы и спады с различной периодичностью и интенсивностью [5]. Данные методы ограничиваются заданными функциями распределения, которые не всегда улавливают критический трафик.

Ряд работ посвящен проблемам связности временных рядов и оценкам автокорреляционных функций, которые позволяют привлечь дополнительные данные, необходимые для выявления аномалий. В частности, в [6, 7] показано, что автокорреляционные функции временных рядов сетевого трафика обладают медленно убывающей зависимостью во всех исследуемых реализациях, т.к. функции имеют фрактальный характер. Анализ автокорреляций наряду со спектральным анализом используется для оценки средних значений, что позволяет выявить скрытую периодичность значений ряда. Однако, указанный метод чувствителен к погрешностям в задании исходных данных и не всегда приводит к заключениям о наличии закономерностей в изучаемом процессе. Изучение энергетических спектров трафика, переданного по протоколу TCP, в работах [6, 8, 9] показало присутствие гармонической компоненты ~5 Гц. Обнаруженное явление выявляет присутствие регулярной детерминированной составляющей в агрегированном сетевом трафике, однако причины появления подобных компонент в спектрах трафика неясны. Для их выявления необходимы стендовые испытания с использованием широкого набора методов

анализа трафика.

Прогнозирование поведения информационной системы требует построения специальных моделей прогноза. Примером часто используемой модели является модель авторегрессии – AR, ARMA, ARIMA, FARIMA. В работе [5] показано, что метод прогнозирования на основе моделей авторегрессии дает лучший результат для процессов со слабо выраженными или отсутствующими фрактальными свойствами. При повышении степени фрактальности прогноз осуществляется на свойствах самоподобных процессов, т.к. он лучше использует корреляционные связи, которые возрастают со степенью фрактальных свойств. Работы по анализу сетевого трафика [6]показывают, что самоподобные процессы лучше всего описываются так называемыми распределениями с «тяжелыми хвостами».

Анализ рассмотренных работ показал, что оценка статистических свойств внешнего трафика не решает задачу обнаружения внутренних аномальных процессов, протекающих в ИС, таких как атаки на оперативную память, работу процессора, каналов, интерфейсы системы (переполнение памяти, SYN – флуд атаки и т д). Методы, основанные на анализе поведения компонент программного обеспечения и осуществляющие контроль поведения ИС на уровне исполняемого кода и на уровне доступа к ресурсам [10], требуют детального описания и привязки к конкретному объекту.

2. Описание модели. Изменение поведения процесса на уровне исполняемого кода приводит к выполнению инструкций, не предусмотренных логикой решаемой задачи, что влечет за собой изменения характера обращения к ресурсам ИС и может быть зафиксировано путем анализа процессов, протекающих в интерфейсах системы [11,12]. Исследование работы ИС в «нормальном» режиме, а также под воздействием атаки позволяет утверждать, что распределения значений частот обращения к разным ресурсам на одном и том же временном отрезке различаются. В связи с этим возникает необходимость описания функционирования системы на основе потоков информации, циркулирующих внутри ИС. Обмен данными между подсистемами ИС можно описать с помощью информационной модели, что позволит описывать (процесс) обмен данными в рамках единого интерфейса, в котором информационную систему S можно представить:

$$S = \langle Struct, Fun \rangle .$$

Структурные компоненты ИС можно представить в виде $Struct = (C, F, Z, T)$, где C — множество подсистем, входящих в S; F

-множество информационных потоков, циркулирующих между подсистемами ИС, Z — множество событий, генерируемых информационными потоками, T — время/набор временных интервалов.

Тогда выполнение набора функций Fun можно рассматривать как обмен информационными потоками между компонентами ИС. При этом каждая функция подсистемы предоставляет другой подсистеме интерфейс представления результатов выполнения функции, при котором на обработку информации расходуется время T. Непосредственно информационный поток $f_i \in F$ ($i = 1,...M$, где M количество потоков) рассматривается как одномерный массив данных в виде числового ряда $\{f_{ij}\}$, заданный в дискретные моменты времени t_j ($j = 1..N$ — интервал между отдельными наблюдениями, N — количество наблюдений). Это позволяет получить набор временных рядов, характеризующих поведение ИС в «нормальном» состоянии во время и после осуществления атаки на ИС.

Для наблюдения за процессом работы ИС введем вектор параметров состояния $Param = (c, f, z, t)$, где c-количество подсистем, задействованных в процессе выполнения функций Fun; f-количество информационных потоков, циркулирующих между подсистемами ИС, z — количество событий, генерируемых информационными потоками, t — момент времени, в который производятся измерения параметров.

Тогда, основываясь на «аномальном» изменении значения вектора $Param$, можно судить не только о наличии или отсутствии атаки, но и построить онтологию, характеризующую тип атаки для различных режимов работы при заданном наборе характеристик подсистем. Определенное сочетание значений $Param$ может свидетельствовать об аномальном поведении, что позволяет принимать решения о выборе режима функционирования. Информационные процессы, связанные с атакой, можно описать в виде: $A = \langle K, Param \rangle$, где K — тип атаки. Если ограничиться простейшей характеристикой обнаружения атаки, достаточно воспользоваться исходными данными для построения порогового значения характеристик ИС, т.е. использовать оценочные средние значения исследуемых временных характеристик подсистем, зафиксированных для m различных режимов работы исследуемого процесса.

Например, для каждого из типов атак K, зафиксированных с по-

мощью превышения порогового значения временного ряда системы S, формируется вектор аномального трафика. Для оценки работы ИС в качестве элементов компоненты *Struct* были выбраны подсистемы «Память» и «Процессор». В этом случае вектор аномального трафика представляется в виде:

$$F_{prp} = \left\langle f_{os}, f_{sp}, f_{pr}, f_{l} \right\rangle,$$

где f_{os} — загрузка ОС; f_{sp} -загрузка сегментов программного кода; f_{pr} — загрузка процессора; f_{l} — поток входных данных (сетевой поток).

Анализ временных рядов, полученных на стенде и включающих объем информационного потока функционирования оперативной памяти (ОП), загрузку процессора, частоту программных и аппаратных прерываний показал, что имеются различия в работе отдельных подсистем при наличии атаки и без нее. Например, графики, представленные на рис. 1,2,3, показали изменения параметров f_{l}, f_{pr}, f_{sp} соответственно при ICMP-флуд атаке начиная с отрезка времени 20:36 по 20:37.

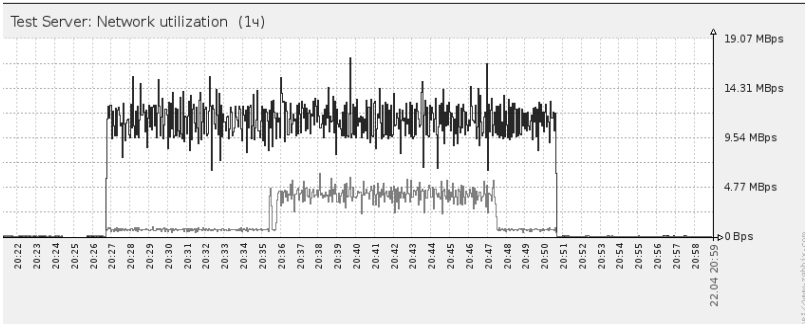

Рис.1 Входящий трафик при ICMP-флуд атаке.

При этом характеристики входного сетевого трафика временного ряда в режиме «нормальной» работы ИС и во время атаки отличаются незначительно. Однако, наличие аномальной активности показывают такие характеристики временных рядов, как объем используемой оперативной памяти, загруженность процессора, наличие программных и аппаратных прерываний. Данные оценки образуют временные ряды с указанием порогового значения для каждого типа атак и могут быть

использованы для проведения градуировки шкалы и прогнозирования возможного влияния выявленной атаки. Эта процедура очень важна как с точки зрения «пропуска» атак при оценке только характеристики порогового значения входного трафика, так и для предотвращения большого числа ложных срабатываний средства обнаружения атак и предотвращение возникновения «Dos атак второго рода».

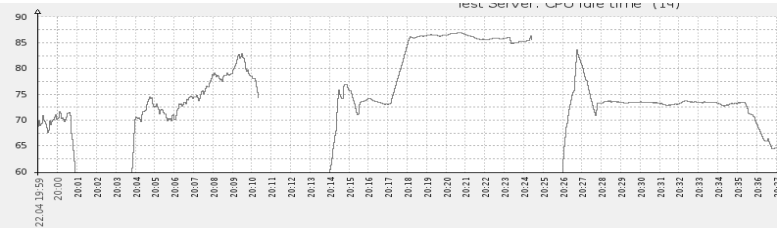

Рис.2. Загруженность процессора при ICMP-флуд атаке.

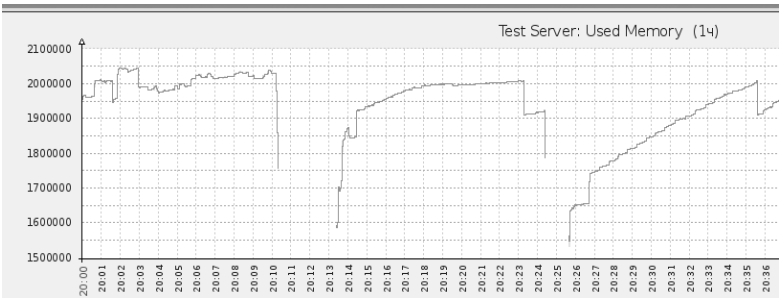

Рис 3. Объем используемой памяти при ICMP-флуд атаке.

3.Заключение. Моделирование поведения информационных потоков показало, что линейные модели не дают адекватной оценки протекающего процесса для критических условий. На основе анализа трафика показана возможность идентификации атаки по пороговому значению, т.е. можно сделать вывод о возможности определения класса применяемых атакующими хостами атак. На основании полученной информации можно предусмотреть использование соответствующих способов противодействия, направленных на борьбу с конкретной атакой.

Литература

1. *Бельков Д.В., Едемская Е.Н., Незамова Л.В.* Статистический анализ сетевого трафика // Наукові праці Донецького національного технічного університету, серія

«Інформатика, кібернетика та обчислювальна техніка»,вып. 13. Донецк: ДонНТУ, 2011. С. 66–75.
2. *Воробьев В.И., Евневич Е.Л., Фаткиева Р.Р.* Моделирование сетевого трафика методом Монте-Карло // Вестник Бурятского государственного университета. 2010. №9. С. 258–262.
3. *Воробьев В.И.* Математическое обеспечение ЭВМ в науке и производстве. Монография Л.: Машиностроение, 1988. 160 с.
4. *Воробьев В. И., Фаткиева Р.Р.* Природа уязвимостей программного кода // Программируемые инфокоммуникационные технологии. 2009. №7–С.53-55
5. *Крюков Ю.А., Чернягин Д.В.* Мониторинг сетевого трафика с регистрацией аномальных событий на основе ГИС-технологий // Геоинформатика. 2009. №2. С. 19–25.
6. *Котенко И.В., Шоров А.В., Нестерук Ф.Г.* Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. 2011. Вып. 18. С.19–73.
7. *Макшанова Л.М., Содномова М.С.* Алгоритм прогнозирования объектов локализуемого трафика в сети БФ ОАО «Ростелеком» // Вестник Бурятского государственного университета, 2011. №.9. С. 99–103.
8. *Мишин К.Н., Фаткиева Р.Р.* Природа сетевых аномалий и их полунатурное моделирование // Труды СПИИРАН. 2007. Вып. 5. С. 260–267.
9. *Репин Д.С.* Анализ и моделирование трафика в корпоративных компьютерных сетях: автореф. дис. … кан. тех. наук: 05.13.01/ Д.С. Репин. – М., 2008. – 143 с.
10. *Петров В.В.* Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия: автореф. дис. … кан. тех. наук: 05.12.13/ В.В. Петров. – М., 2004. – 20 с.
11. *Фаткиева Р.Р. Помецко В.В.* Метод идентификации уязвимостей программного кода // Программируемые инфокоммуникационные технологии. 2009. №7–С.55-59
12. *Leland W.E., Taqqu M.S., Willinger W., Wilson D.V.* On the self-similar nature of Ethernet traffic (extended version). IEEE/ACM Transactions of Networking. 1994. № 2. С.1-15.
13. *Chandra K., You C., Olowoyeye G., Thompson C.* Non-linear Time-Series Models of Ethernet Traffic // CACT, Tech. Rep., June 1998.

Фаткиева Роза Равильевна — канд. техн. наук; старший научный сотрудник лаборатории информационно-вычислительных систем СПИИРАН. Область научных интересов: моделирование информационных систем. Число научных публикаций — 25. rikki2@yandex.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-4369, факс +7(812)328-4450.

Fatkieva Rosa Ravilievna — researcher, Laboratory of Computer and Informational Systems, SPIIRAS. Research interests: modeling of information systems. The number of publications — 8. atiskov@gmail.com; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-4369, fax +7(812)328-4450.

Рекомендовано лабораторией информационно-вычислительных систем СПИИРАН, заведующий лабораторией Воробьев В.И, д-р техн. наук, проф.
Статья поступила в редакцию 21.05.2012.

РЕФЕРАТ

Фаткиева Р.Р. **Модель обнаружения атак на основе анализа временных рядов.**

Приводится сравнительный анализ методов исследования входных, выходных и внутренних трафиков информационной системы. Показано, что поведение информационных систем носит нелинейный характер, основные сетевые протоколы, присутствующие в информационных системах порождают хаотические структуры, нелинейное поведение которых заложено в их алгоритмах (например, механизмы «медленного старта», борьбы с перегрузками в вычислительных сетях). Оценка статистических свойств внешнего трафика не решает задачу обнаружения внутренних аномальных процессов, протекающих в ИС, таких как атаки на оперативную память, работу процессора, каналов, интерфейсы системы (переполнение памяти, SYN- флуд атаки и т.д.). Методы, основанные на анализе поведения компонент программного обеспечения и осуществляющие контроль поведения ИС на уровне исполняемого кода и на уровне доступа к ресурсам, требуют детального описания и привязки к конкретному объекту. В критических случаях изменение поведения вычислительного процесса на уровне исполняемого кода приводит к выполнению инструкций, не предусмотренных логикой решаемой задачи. Изменения характера обращения к ресурсам ИС может быть зафиксировано путем регистрации событий, протекающих в ИС.

Предложен подход к обнаружению атак отказа в обслуживании, основывающийся на анализе временных рядов. Моделирование поведения информационных потоков показало, что линейные модели не дают адекватной оценки протекающего процесса для критических условий. Показана возможность идентификации атаки по пороговому значению и определения класса на основе анализа трафика. На основании полученной информации можно предусмотреть использование соответствующих способов противодействия, направленных на борьбу с конкретной атакой.

SUMMARY

Fatkieva R.R. **Model of attack detection on the basis of time series analysis.**

Research methods of information system input, output and inner traffic are analyzed in comparison. Information systems behavior is shown to be non-linear, main network protocols of information systems are proved to generate chaotic structures, non-linear behavior of the latter is determined by their algorithms (for example, “slow start” mechanisms, those of overload control, etc.). Estimations of external traffic statistics cannot solve the problem of detection of internal abnormal processes in the information systems such as storage, processor, channels and interfaces attacks (storage overflow, SYN- and flood- attacks and others). Methods based on the program components behavior analysis, being applied at the code and resource access levels, require detailed description and attachment to certain object. In crucial cases changes in the behavior of computer process at the code level result in the implementation of instructions being unspecified by logic of the problem under fulfillment. Changes in the manner of resource access can be fixed by means of logging the events taking place in the information system. Approach to denial-of-service attack detection on the basis of time series analysis is proposed. Modeling of information flows behavior make it obvious that linear models are unable to provide adequate estimations of the process in the critical conditions. Feasibility of attack identification by means of threshold value method and its class determination by traffic analysis are demonstrated. On the basis of collected information there is a possibility to use appropriate techniques to reduce specific attack.