Записки научных
семинаров ПОМИ
Том 352, 2008 г.

К. Н. Мишин

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ АНОМАЛЬНЫХ ЯВЛЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Природа аномального поведения информационно-вычислительных систем связана, прежде всего, с чрезвычайной сложностью объекта, который включает в себя огромное количество компьютерных устройств, систем передачи данных на основе системы взаимосвязанных протоколов и коллективной работы большого числа пользователей (и системных администраторов). Работа таких систем может быть описана системой

$$\dot{x} = f(x), \;\; x \in \mathbb{R}^N$$

нелинейных дифференциальных уравнений в пространствах большой размерности. Для большинства сетевых протоколов (к примеру, таких, как TCP/IP) нелинейное поведение заложено в самих их алгоритмах, к примеру, в механизмах "медленного старта", борьбы с перегрузками в сетях и UDP на масштабе полного обращения информационных пакетов (Round Trip Time).

В работе [7] показано, что основные сетевые протоколы порождают хаотическую структуру сетевого трафика и поведение систем может быть описано при помощи теории динамических систем. В этой работе для описания поведения информационно-вычислительной системы в качестве ее параметров, значение каждого из которых является координатой x_i фазового пространства динамической системы, были выбраны: скорость передачи информации (в Мбит/с), время передачи информации (мс), количество переданных информационных пакетов для TCP трафика. Оказалось, что в фазовом пространстве такой (трехмерной) системы имеется притягивающее множество со сложной структурой.

Вообще говоря, размерность фазового пространства соответствующей динамической системы может оказаться гораздо большей трех. В качестве параметров в модели, описывающей поведение информационно-вычислительной системы, можно выбирать:

- пропускную способность канала передачи (Мбит/с);
- объем передаваемой информации (бит);
- размер буфера приема/передачи (бит)
- количество сетевых узлов в инфраструктуре сети;
- количество пользователей;
- параметрические характеристики сетевых протоколов.

Для моделирования сетевых аномалий нужно прежде всего провести их таксономию, что позволит уточнить необходимость введения параметра, позволяющего определить начало сетевой атаки (в частности, этот анализ позволит установить размерность фазового пространства).

Анализ и выявление природы конкретного класса атак основывается на анализе цикла развития и воздействия информационной атаки или угрозы. Так, например, атаки отказа в обслуживании зачастую классифицируются как парализующие атаки и угрозы, которые уменьшают пропускную способность каналов передачи данных, выводят из строя различные сетевые сервисы и представляют собой угрозы, аккумулирующие аномальные явления на всех фазах динамики развития и воздействия угрозы информационной безопасности.

Для выявления и идентификации признаков атаки был проведен полунатурный эксперимент. В ходе эксперимента проводилось сравнение различного рода сетевого трафика атак “отказа в обслуживании” с нормальным трафиком глобальной вычислительной сети. Эксперимент показал, что сетевой трафик атаки отличается существенным образом от нормального сетевого трафика. Результатом эксперимента являются сравнительные графики, позволяющие обнаружить сетевую атаку на фоне легального трафика. Значения критически значимых параметров, указывающих на сетевые атаки, позволили реконструировать фазовый портрет системы. В результате удалось лучше понять закономерности развития различного типа атак и повысить эффективность обнаружения атак “отказа в обслуживании”.

В исследуемых атаках можно выделить следующие фазы: **probe** – сканирование узлов (3–4-й уровень модели открытых систем); **penetrate** – механизм проникновения в информационную систему; **persist** – внедрение и вредоносное воздействие на информационную систему; **propagate** – механизм внедрения атаки отказа в систему; **paralyze** – парализация работы системы на неопределенное время.

Для реализации эффективного механизма раннего обнаружения атак и, соответственно, угроз информационной безопасности, необходимо иследовать механизмы *зарождения, развития, завершения* атаки. Анализ представленных в таблице 1 (приведенной в конце работы) существующих механизмов защиты показывает, в частности:

- слабость механизма принятия решения в случае появления потенциальной угрозы;
- неэффективность существующих сигнатурных статистических систем обнаружения вторжений, в особенности при появлении неизвестной аномалии;
- применяемые методы моделирования не вскрывают сущности атак, поскольку имеющиеся методы не позволяют оценить характер динамики потенциальной аномалии,

таким образом, сопоставление классов атак и средств защиты показывает их слабую эффективность.

Естественным подходом является изучение поведения динамической системы на полунатурном стенде, в результате чего мы можем получить реальные траектории рассматриваемой системы. Стенд представляет собой натурную модель исследования трафика. Его структура моделирует работу участка глобальной сети *Интернет* и состоит из трех основных компонент:

– атакующая сеть, состоящая из n компьютеров;

– атакуемая сеть, состоящая из k компьютеров;

– телекоммуникационное оборудование;

– программно-аппаратный комплекс для анализа атак и аномалий.

Атакующий хост генерирует паразитный трафик, моделирующий исследуемую атаку. Трафик поступает на концентратор, направляющий его далее на атакуемый хост и хост–анализатор. Оба сегмента подключены к сети Интернет через порты *Fast Ethernet*, распоряжении каждого из которых имеется канал с пропускной способностью 100 Мбит/с. Анализатор сканирует проходящий через него трафик атаки и сохраняет его на жестком диске для последующей обработки.

В ходе исследования поведения сетевого трафика были собраны 5 дампов: дамп легального трафика; дампы трафиков атак SYNflood, TCPflood, Smurf и DoomDNS на базе следующих программных элементов и сервисов.

Атакующий хост. Операционная система FreeBSD 6.1; используемые утилиты: средство аудита сети Packit 1.0, приложение, позволяющее произвести атаку DoomDNS–Dnsflood.pl, утилита Apache server benchmarking tool для тестирования производительности HTTP сервера AB.

Атакуемый хост. Операционная система FreeBSD 4.11; сервисы, необходимые для исследования: HTTP сервер Nginx 0.4.12 и сервер доменных имен Bind 9.3.3.

Хост–анализатор. Операционная система FreeBSD 6.1; используемая утилита: TcpDump.

Выявление природы описанных атак с целью их ранней идентификации требует построение соответствующего фазового пространства, координатами в котором являются параметры, характеризующие поведение системы. Другими словами, необходимо выбрать такие параметры, изменение значений которых говорит о происходящих критических изменениях трафика. Следует отметить, что многие его характеристики зависят от времени; отслеживая их поведение, можно сделать вывод о потенциальной аномалии или угрозе информационной безопасности. При этом критические значения (при достижении которых можно говорить об угрозе) параметров будут различными для разных типов атак. В следующей таблице приведены выбранные параметры.

Параметры атаки	**SYN**	**Flood**	**Smurf**	**DDNS**
Количество (SYN – ACK) пакетов в секунду	+	+		
Количество ТШП пакетов в секунду	+	+		
Максимальное число source IP с одинаковым числом TTL в секунду	+		+	+
Количество различных source IP в секунду	+			
Количество различных source PORT в секунду	+	+		
Максимальное число различных портов отправителя для каждого IP отправителя в секунду		+		
Количество ICMP (ECHO reply – ECHO request) в секунду			+	

В качестве примера приведем результаты моделирования для атаки Smurf. В следующей таблице приведены значения ICMP-пакетов, характерных для этой атаки.

Параметры	**Легальный график**	**Трафик атаки**
Пороговое значение	0	
Среднее арифметическое	502,1722	
Спектральная плотность	0	451955

Таким образом, при легальном трафике значение числа ICMP-пакетов равно нулю (см. рис. 1).

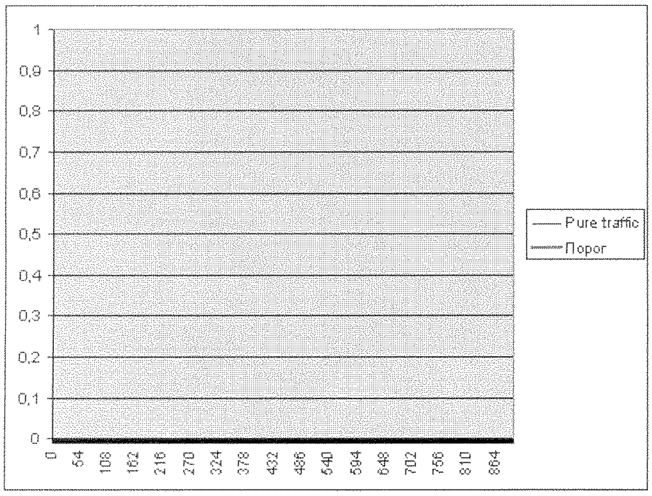


Рис. 1.

На следующей диаграмме показана динамика этого параметра при атаке (см. рис. 2).

В отличие от предыдущего параметра, значения максимального числа source IP с одинаковым числом TTL в секунду отличны от нуля и при легальном трафике. Динамика этого параметра при легальном трафике (см. рис. 3).

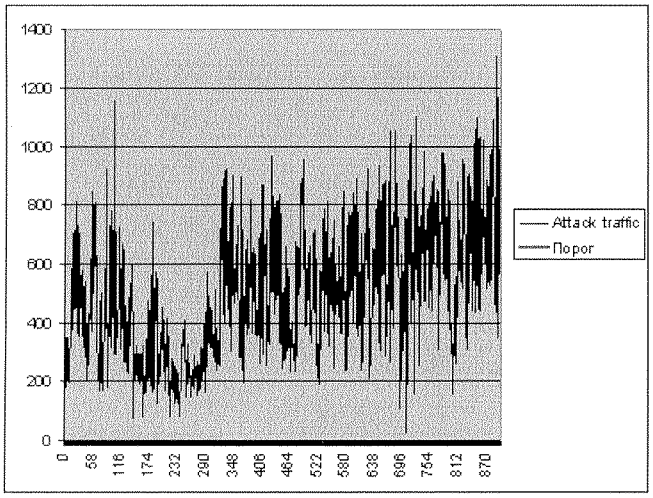


Рис. 2.

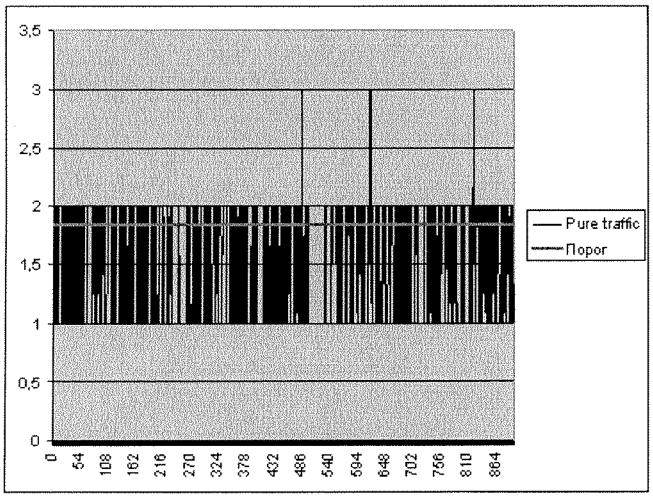


Рис. 3.

Динамика параметра при атаке Smurf (см. рис. 4).

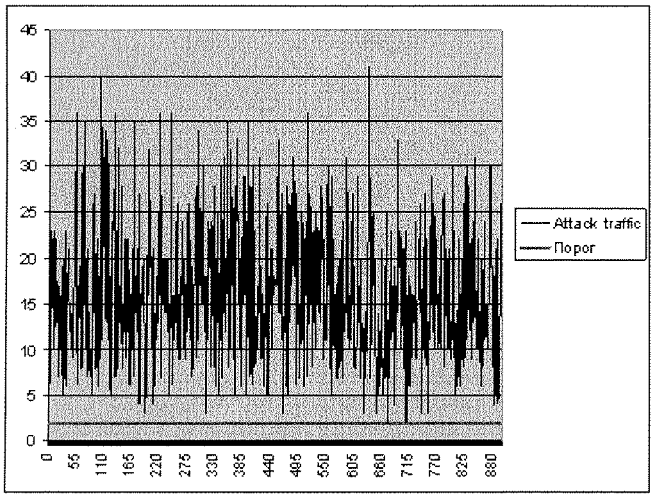


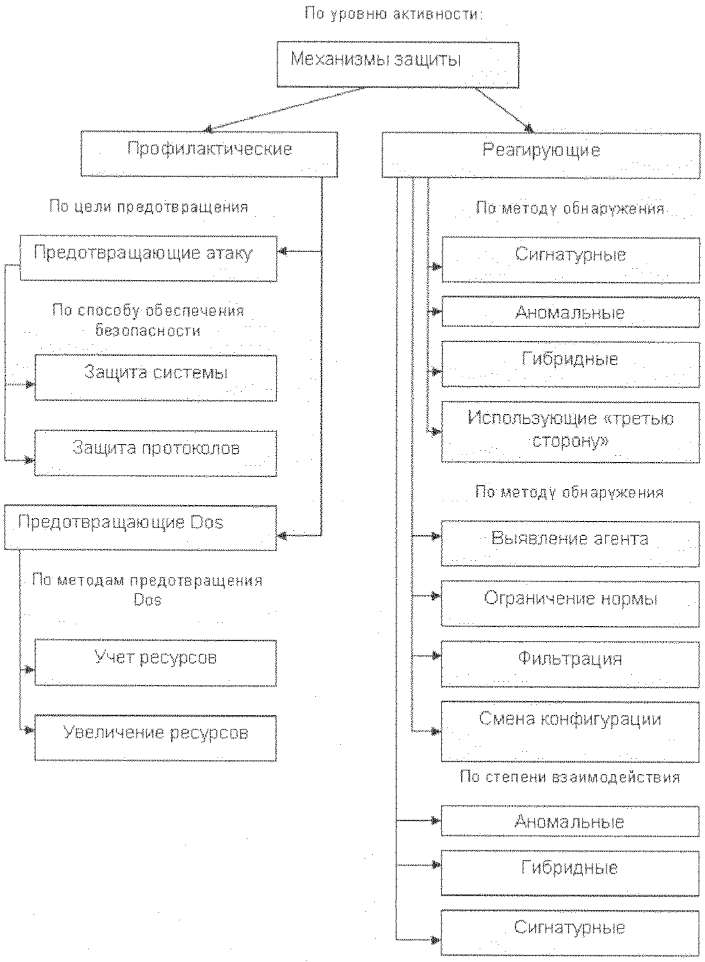
Рис. 4.

Параметры	**Легальный график**	**Трафик атаки**
Пороговое значение	1,845333	
Среднее арифметическое		502,1722
Спектральная плотность	1384	14565

Полученные в результате моделирования данные показывают

что, несмотря на хаотичную динамику систему даже при легальном трафике, существует различие между значениями параметров, которое дает возможность судить о начавшейся атаке,

однако имеется лакуна между пороговыми и оценочными их значениями, из чего следует необходимость дальнейшей градуировки для предотвращения ложных срабатываний средств защиты.



Литература

1. В. Г. Олифер, Н. А. Олифер, *Компьютерные сети. Принципы, технологии, протоколы*. СПб, Питер (2001). 356 с.
2. И. В. Котенко, М. В. Степашкин, В. С. Богданов, *Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников*. Проблемы информационной безопасности. Компьютерные системы (2005). С. 65.

3. В. И. Воробьев, Е. П. Румянцева, Р. Р. Фаткиева, *Оценка эффективности инвестиций в информационую безопасность образовательных технологий.* Труды РГПУ, СПб (2007). С. 47
4. Г. Г. Малинецкий, А. Б. Потапов, А. В. Подлазов, *Нелинейная динамика. Подходы, результаты, надежды.* УРСС (2006). 279 с.
5.] Г. Г. Малинецкий, А. Б. Потапов, *Нелинейная динамика и хаос (Основные понятия).* УРСС (2006). 275 с.
6. J. Mirkovic, J. Martin, and P. Reither, *A Taxonomy of Ddos Attacks and Ddos Defence Mechanisms.* Computer Science Department, University of California, Los Angeles. Technical Report 020018. 8 p.
7. M. Boda, A. Veres, *The Chaotic Nature of TCP Congestion Control. Traffic Analysis and Network Performance Laboratory.* Budapest (2001). 7 p.
8. W. Ditto, T. Mukanata, *Principles and Applications fo Chaotic Systems.* Comm. of the ACM (1995, November). p. 12–24.

Mishin K. N. The imitation modelling of anomalies in computer nets.

The network condition may be described by a set of configuration parameters. Introduced method consists in marking some parameters in order to detect the on-going attack traffic. The results of the modelling are given.

С.-Петербургский государственный электротехнический университет (ЛЭТИ)

E-mail: kmishin@ametist.spb.ru

Поступило 28 января 2008 г.