В.А. Артамонов
Россия, г. Ставрополь, Ставропольский государственный университет

ОБНАРУЖЕНИЕ СЕТЕВЫХ АНОМАЛИЙ ЧЕРЕЗ РЕКОНСТРУКЦИЮ МОДЕЛИ СЕТЕВОГО ТРАФИКА

В настоящее время число факторов, негативно влияющих на безопасность информационных процессов, резко возросло. Злоумышленников все больше интересует кража пользовательской информации через организацию эпидемий вирусов и новых атак. Для этих целей все чаще используются многочисленные группы зараженных компьютеров, так называемые «ботнет» сети. Разработчики вредоносных программ активно работают над повышением технологичности своих разработок и улучшением методов сокрытия присутствия в системе [1]. Это приводит к тому, что полностью препятствовать действиям злоумышленников в информационных системах невозможно. Поэтому для обеспечения необходимого уровня безопасности наиболее актуальны направления исследований, связанные с разработкой систем обнаружения вторжений.

На сегодняшний день в информационной безопасности понятие системы обнаружения вторжений (СОВ) употребляется в широком смысле. Методы обнаружения атак принято разделять на методы обнаружения аномалий и методы обнаружения злоупотреблений. В последних методах используется сигнатурный анализ для определения факта воздействия на систему. Этот метод сходен с работой антивируса – каждое событие вторжения имеет свое описание в базе СОВ. Системы этого типа эффективны при обнаружении известных атак и так же, как и антивирусное программное обеспечение, сигнатурная СОВ эффективна настолько, насколько хороша ее база сигнатур.

Главными преимуществами систем обнаружения аномалий (СОА) являются отсутствие шаблонов поиска и способность к обнаружению новых атак. Это предопределило бурное развитие СОА в последние годы. Наиболее распространенными методами обнаружения сетевых аномалий являются [2]:

- моделирования правил;
- конечных автоматов;
- сигнатурный;
- статистический.

Для любого из вышеперечисленных методов необходимо наличие данных для обучения, прежде чем можно будет запускать СОА в эксплуатацию. Необходимым требованием для тренировочных данных является отсутствие каких-либо атак, иначе СОА будет неспособна обнаруживать атаки, которые были в обучающих данных. Наличие несвойственных аномалий в тренировочном трафике также может быть причиной увеличения количества ложных срабатываний детектора аномалий, когда «нормальный» трафик маркируется как аномалия и возможная атака. Поэтому актуальной является задача разработки методов выявления аномалий, основанных на автоматическом построении модели поведения системы.

Для решения этой задачи предлагается использовать методику реконструкции математической модели динамической системы по временным рядам показателей состояния сети. Это позволит по записи временного ряда показателей одного из параметров системы восстановить сложность и некоторые характеристики (например, динамику) всей системы. Отслеживание изменения параметров реконструированной модели сможет выявлять атаки в наблюдаемой системе.

Задача выявления аномалий предложенным методом выполняется в три шага:

1. Выбор оптимальных параметров реконструкции для восстановления аттрактора системы и выполнение реконструкции.

2. Идентификация параметров системы дифференциальных уравнений, описывающих восстановленный аттрактор.

3. Мониторинг изменения параметров уравнений реконструированной модели.

Объектом анализа являются временные ряды из количества пакетов, прошедших через сетевой интерфейс за 1 секунду.

Для реконструкции аттрактора динамической системы по временному ряду экспериментальных данных $\{x\}$ необходимо решить проблему выбора оптимальных параметров реконструкции: временной задержки τ и размерности вложения m. Результат реконструкции полностью зависит от выбора обоих параметров. Оценка оптимальных $\{m_{opt}, \tau_{opt}\}$ выполняется с помощью показателя дифференциальной энтропии [3], так как этот метод, в отличие от альтернативных, позволяет получить оба параметра одновременно.

Дифференциальная энтропия используется для оценки «беспорядка» с использованием плотности распределения вероятностей $p(x)$ данных. Из-за гибкости по отношению к размерности используемых данных очень часто используется оценка для дифференциальной энтропии, предложенная Ю.В. Козаченко и Г.М. Леоненко:

$$H(x) = \sum_{j=1}^{N} \ln(N\rho_j) + \ln 2 + C_E \,. \qquad (1)$$

В формуле 1 N – длина временного ряда, ρ_j – Евклидова дистанция от j-го реконструированного вектора к его ближайшему соседу и C_E (≈ 0.5772) – постоянная Эйлера. Дифференциальная энтропия для вложения временного ряда $\{x\}$, размерности вложения m, временной задержки τ обозначается как $H(x, m, \tau)$. $H(x, m, \tau)$ будет обратной мерой структуры в фазовом пространстве.

Набор оптимальных параметров $\{m_{opt}, \tau_{opt}\}$ позволяет получить фазовый портрет, наиболее полно отражающий динамику в реальной системе. Таким образом, оптимальный портрет имеет минимальную дифференциальную энтропию (минимальный «беспорядок») и отклонение от оптимальных $\{m_{opt}, \tau_{opt}\}$ приводит к увеличению «беспорядка». Поэтому для нахождения оптимального набора параметров необходимо минимизировать $H(x, m, \tau)$.

Для компенсации неустойчивости уравнения (1) по отношению к изменению размерности, в [3] было рекомендовано использовать некоторое количество «суррогатных» сигналов, полученных из $\{x\}$. Необходимое количество N_s таких сигналов $\{x_{s,i}\}, i = 1, ..., N_s$, генерируется случайными перестановками в оригинальном временном ряде. В этом случае распределение сигнала не меняется и корреляция внутри ряда остается случайной. В результате получается новый «обеленный» сигнал с распределением, идентичным исходному ряду $\{x\}$. Дифференциальная энтропия вычисляется для реконструированных временных рядов экспериментальных данных и для суррогатов по формуле (1) для постоянно увеличивающихся m и τ. Чтобы определить оптимальные параметры реконструкции, необходимо оптимизировать следующее отношение:

$$I(m,\tau) = \frac{H(x,m,\tau)}{< H(x_{s,i},m,\tau) >_i} \quad , \qquad (2)$$

где $< \cdot >_i$ означает среднее значение выражения по i. В табл. 1 представлены результаты оценки оптимальных параметров реконструкции для 10 временных рядов длиной 200 точек, составленных по тестовым наборам данных MIT Lincoln Laboratory [4].

Таблица 1

Оптимальные параметры реконструкции

	R_{ent}	
	m_{opt}	τ_{opt}
1	2	16
2	2	12
3	2	23
4	3	15
5	2	28
6	5	14
7	2	42
8	2	34
9	2	19
10	2	33

Обработка всех данных за 4-ю и 5-ю недели наблюдений от MIT Lincoln Laboratory и реальных данных для канала доступа в Интернет Ставропольского государственного университета позволяет сделать вывод, что примерно в 80% случаев реконструируемый аттрактор будет иметь размерность 2. Это значит, что для его описания потребуется система из 2 дифференциальных уравнений второй степени вида:

$$\dot{x}_i = \sum_{k=1}^{K} c_{i,k} F_{i,k}(x_1, x_2, ..., x_D) \, , \qquad (3)$$

где $i = 1,..., D$, D – степень уравнений, K – количество уравнений и $c_{i,k}$ – параметры, которые надо найти. Идентификация параметров уравнений (3) выполняется с помощью метода наименьших квадратов. Для случая из 2 уравнений необходимо найти значения 18 параметров.

Проверка предложенного метода выполнялась по временному ряду для 5 минутного отрезка тренировочных данных MIT Lincoln Library. Реконструкция уравнений производилась по последним 200-м точкам от момента наблюдений. График изменения параметров во времени представлен на рис.1. Ось абсцисс – порядковый номер параметров (здесь 10-ый – 18-ый параметры – соответственно 1-й – 9-й параметры второго уравнения), ось ординат – порядковый номер реконструкции и ось аппликат – значение параметров.

Через 1 минуту после начала мониторинга наблюдается резкое изменение всех параметров уравнений, что сигнализирует об обнаружении атаки. Этот момент точно совпадает с данными Lincoln Library о том, что в это время была выполнена атака вида mailbomb.

Таким образом, предложен новый метод обнаружения сетевых аномалий по временным рядам одного из показателей состояния сети, который не требует наличия данных для обучения системы обнаружения аномалий.

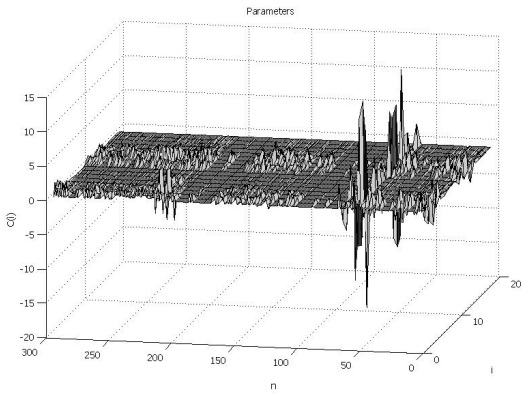

Рис. 1

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гостев А.*, Современные информационные угрозы, I квартал 2007, http://www.viruslist.com/ru/analysis?pubid=204007545

2. *Thottan M. and Ji C.*, Anomaly Detection in IP Networks, IEEE transactions on signal processing, Vol. 51, No. 8, 2003

3. *Gautama T., Mandic D., Van Hulle M.*, A differential Entropy based method for determining the optimal embedding parameters of a signal, 2003

4. MIT Lincoln Library DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/IST/ideval/data/data_index.html

П.П. Кравченко, Н.Ш. Хусаинов, А.Н. Шкурко
Россия, г. Таганрог, Технологический институт ЮФУ

МЕТОДЫ ОГРАНИЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРЕДАВАЕМЫМ МЕДИАДАННЫМ В АРХИТЕКТУРЕ СИСТЕМЫ МНОГОСТОРОННЕЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ «ДЕЛЬТА-КОНФЕРЕНЦИЯ»

В последнее время все большее распространение в задачах управления бизнесом получают системы многосторонней видеоконференцсвязи (ВКС). Это связано с тем, что эффект от аудиовизуального общения значительно выше, чем при общении по телефону, а тем более посредством электронной почты и т.п. Во время сеанса видеоконференцсвязи имеется возможность наблюдать реакцию собеседника, что может быть особенно важно в деловых переговорах. Но, несмотря на явные преимущества подобных систем, не многие компании активно используют их в своей работе. Это связано, прежде всего, с тем, что, во-первых, существующие на рынке системы отличаются дороговизной, и, следовательно, могут быть по карману только достаточно крупным компаниям, во-вторых, существующие системы зачастую отличаются низким соотношением цена/качество и, наконец, большинство известных программных систем ВКС предполагают взаимодействие между пользователями через централизованный сервер компании-производителя (через Интернет). Также этот выделенный сервер (аппаратно-программный комплекс) может быть приобретен отдельно, но его стоимость крайне высока. Следует также