УДК 004.056 + 621.391 + 004.7.056 Вестник УрФО № 2(24) / 2017, с. 18–24

Агафонов А. В.

МОДЕЛЬ СЕТЕВОЙ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ В ЗАДАЧЕ ТЕСТИРОВАНИЯ ЕГО ЗАЩИЩЕННОСТИ ОТ СЕТЕВЫХ КОМПЬЮТЕРНЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

В статье представлена модель сетевой среды функционирования телекоммуникационного оборудования, предназначенная для решения задачи тестирования его защищенности от сетевых компьютерных атак типа «отказ в обслуживании». Указанная модель позволяет отразить в синтезируемом с ее применением тестовом сетевом трафике свойство самоподобия, структуру и статистические характеристики трафика заданной сетевой среды, в которой производится эксплуатация образца телекоммуникационного оборудования, при проведении направленных на него сетевых компьютерных атак типа «отказ в обслуживании».

Ключевые слова: *тестирование, телекоммуникационное оборудование, отказ в обслуживании, сетевой трафик, модель.*

Agafonov A.

NETWORK ENVIRONMENT MODEL INTENDED FOR TESTING THE IMMUNITY OF TELECOMMUNICATION EQUIPMENT AGAINST DENIAL OF SERVICE NETWORK ATTACKS

The article describes telecommunication equipment network environment model intended for testing its immunity against denial of service network attacks. The model allows to reflect the self-similarity property, structure and statistical parameters of traffic from a given network environment in test network traffic synthesized with its application.

Keywords: *testing, telecommunication equipment, denial of service, network traffic, model.*

Одним из важных этапов аудита информационной безопасности компьютерных сетей является оценка их защищенности от сетевых компьютерных атак (СКА) типа «отказ в обслуживании». При этом оценке должна подвергаться не только серверная инфраструктура, но и входящее в их состав телекоммуникационное оборудование (ТКО) — коммутаторы и марш-рутизаторы, — так как успешная реализация направленных на него атак может привести к одновременному нарушению штатного информационного взаимодействия множества узлов сети и нанести значительный ущерб.

Направленные на ТКО СКА типа «отказ в обслуживании» в большинстве случаев производятся с использованием корректного сетевого трафика (СТ), соответствующего спецификациям используемых протоколов передачи данных, параметры которого отличаются от штатного СТ лишь количественно. Также особенностью рассматриваемых СКА является то, что они реализуются на уровнях модели OSI не выше транспортного[1].

Наиболее широко применяемым методом оценки защищенности ТКО от СКА типа «отказ в обслуживании» является его натурное тестирование в изолированной сетевой среде с применением синтезированного тестового СТ, имитирующего комбинацию штатного информационного взаимодействия защищаемой компьютерной сети и атакующего воздействия. При тестировании ТКО осуществляет пересылку данного СТ, в процессе которой производится оценка его способности обеспечить заданный требованиями компьютерной сети уровень доступности информации, численно выражающийся как совокупность среднего значения задержки передачи пакетов, ее неравномерности, называемой также джиттером, и относительной доли потерь пакетов.

При высокой интенсивности информационного взаимодействия между узлами сети распределение пакетов, поступающих в ТКО, не является равномерным, а имеет выраженный характер пульсации, что повышает вероятность превышения его пропускной способности, которое приводит к потере и задержкам пакетов в процессе передачи. Существующие исследования показывают, что данная особенность СТ компьютерных сетей связана с проявлением им свойства *самоподобия*, то есть сохранения динамики изменения его параметров вне зависимости от выбранных масштабов временной оси[2].

Непосредственной характеристикой наличия самоподобия является параметр *Хер-*

cma (Hurst parameter) χ, являющийся общепринятым критерием оценки самоподобия СТ и рассчитываемый по формуле:

$$\chi = \frac{ln(R/S)}{ln(N)} .$$

Для вычисления χ используются следующие величины:

N — количество отсчетов изучаемой случайной величины;

X_{avg} — среднее значение случайной величины:

$$X_{avg} = \frac{1}{N}\sum_{i=1}^{N} x_i ,$$

где x_i — *i*-й отсчет случайной величины;

S — среднеквадратичное отклонение случайной величины:

$$S = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - X_{avg})^2} ;$$

D — накопленное отклонение:

$$D = \left\{\sum_{i=1}^{N}(x_i - X_{avg})\right\}_{i=1}^{N} ;$$

R — размах накопленного отклонения:

$$R = max(Z) - min(Z) .$$

Значения χ находятся в пределах от 0,5 до 1 для значений интенсивности передачи данных и межпакетного временного интервала. Значение этого коэффициента в области 0,5 указывает на отсутствие самоподобия, а близость к 1 — на проявление данных свойств.

Кроме того, современные исследования показали, что СТ, передаваемый в ТКО с идентичной интенсивностью, но имеющий различную структуру потоков данных (например, количество одновременно взаимодействующих узлов и доли пакетов, генерируемых инициаторами потоков) или их статистические характеристики (такие как средние значения, дисперсия значений межпакетных временных интервалов и размеров пакетов), может оказывать различное влияние на величину задержки передачи данных и потери пакетов при их обработке ТКО[3].

Таким образом, для обеспечения адекватности результатов тестирования ТКО необходимо синтезировать тестовый СТ, обладающий свойствами самоподобия, а также структурой и статистическими характеристиками потоков данных, сходными с параметрами СТ, циркулирующего в условиях СКА типа «отказ в обслуживании» в сетевой среде, где функционирует рассматриваемый образец ТКО.

Для решения данной задачи была разработана математическая модель сетевой среды функционирования (ССФ) ТКО, позволяющая отразить указанные параметры в синтезируемом с ее помощью СТ.

Топология моделируемой сетевой среды в рамках модели описывается с помощью следующих параметров:

– множества узлов сетей H, где n_h — их количество:

$$H = \{h_i\}_{i=1}^{n_h};$$

– множества сетей W, где n_w — их количество:

$$W = \{w_i \mid w_i \subseteq H\}_{i=1}^{n_w};$$

– вектора Z, где n_z — количество сетевых интерфейсов (СИ) ТКО, а z_i — множество сетей, для которых существует маршрут передачи данных между входящими в них узлами и i-м СИ ТКО, не содержащий данный образец ТКО в качестве промежуточного узла:

$$Z = \{z_i \mid z_i \subseteq W\}_{i=1}^{n_z}.$$

Статистическое распределение логических соединений между взаимодействующими сетевыми узлами в рамках модели рассматривается как совокупность потоков, где под термином поток подразумевается множество пакетов, создаваемых в процессе обмена данными между двумя конечными узлами сети с использованием протокола транспортного уровня или управления сетью в течение определенного интервала времени.

Каждый из потоков определяется параметрами, характеризующими логическое соединение между взаимодействующими сетевыми узлами:

– идентификатором типа потока, определяющим используемый протокол транспортного уровня или управления сетью — $a \in \{\overline{1\ n_a}\}$, где n_a — количество различных типов потоков;

– сетевыми адресами $h_1, h_2 \in H$ узла-инициатора процесса передачи данных (УИ) и узла, взаимодействующего с инициатором (УВ);

– номерами портов (для протоколов транспортного уровня) или типами генерируемых сообщений (для протоколов управления сетью) $p_1, p_2 \in \{\overline{1\ n_p}\}$ УИ и УВ, где n_p — предельное значение данного параметра.

Статистические характеристики СТ, связанные с размером и распределением сете-

вых пакетов во времени внутри каждого из логических соединений, рассматриваются как случайные величины и задаются своими функциями распределения (ФР) 4.

Определены векторы следующих статистических характеристик:

– не связанных с направлениями передачи данных:

$$C_0 = \langle F_h, F_f \rangle,$$

где F_h — ФР вероятности события генерации пакета УИ или УВ, а F_f — ФР длительности потока;

– связанных с направлениями передачи от УИ к УВ:

$$C_1 = \langle F_{l1}, F_{t1} \rangle,$$

– связанных с направлениями передачи от УВ к УИ: $C_2 = \langle F_{l2}, F_{t2} \rangle,$

где F_{li} — ФР размера пакета, F_{ti}, $i = \overline{1,2}$ — ФР промежутка времени между началами передач двух последовательных пакетов.

В компьютерных сетях, как правило, можно выделить множества взаимодействующих серверов и клиентов. Характер взаимодействия между ними может быть описан с использованием термина группа потоков.

Группа потоков — множество потоков СТ, циркулирующего между определенными множествами узлов-клиентов $H_1 \subseteq H$ и узлов-серверов $H_2 \subseteq H$. Данная группа может быть описана типом потока a, используемого для реализации взаимодействия, ФР F_{h1} индекса УИ, ФР F_{h2} индекса УВ, а также номерами портов транспортного уровня или типами сообщений p_1 и p_2, используемых соответственно УИ и УВ, а также векторами статистических параметров СТ C_0, C_1 и C_2.

Структура сетевого взаимодействия всех элементов ИТСиС защищаемого объекта отражена в модели с помощью вектора $\langle G_i \rangle_{i=1}^{n_g}$ групп потоков, где каждая из которых G_i может быть описана выражением:

$$G_i = \langle a, F_{h1}, F_{h2}, p_1, p_2, C_0, C_1, C_2 \rangle.$$

Компонентами модели являются также ФР F_g вероятности события генерации в СТ потока каждой из n_g групп, а также ФР F_c количества инициируемых в сети потоков в единицу времени.

Таким образом, модель M ССФ ТКО определяется следующим выражением:

$$M = \langle H, W, Z, \langle G_i \rangle_{i=1}^{n_g}, F_g, F_c \rangle.$$

Блок-схема алгоритма синтеза тестового СТ на основе параметров модели приведена на рис. 1.

В процессе его работы для определении характеристик СТ применяется функция, обозначенная как *Random*, возвращающая значение случайной величины, подчиняющейся заданной ФР.

Для синтеза пакетов потоков TCP, UDP и ICMP используются одноименные процедуры, исходными данными которых являются:

j — уникальный идентификатор пакета;

h_1 — момент времени начала потока;

h_2 — момент времени завершения потока;

t_0 — момент времени начала потока;

t_1 — момент времени завершения потока;

G_g — группа потока.

При запуске процедур производится извлечение статистических параметров C_0, C_1 и C_2 группы потоков G_g. Длительность потока определяется на основе параметра F_f, отправители синтезируемых пакетов — на основе F_h, длины пакетов и межпакетные интервалы — с помощью F_{ll} и F_{tl} или F_{l2} и F_{t2} в зависимости от узла-отправителя. Заголовки пакетов генерируются в соответствии с наименованием процедуры. В поле Identication заголовка IP и область данных прикладного уровня помещается уникальный числовой идентификатор пакета.

При этом в процессе синтеза потока TCP корректно устанавливаются номера последовательности (TCP sequence number), подтверждения (TCP acknowledgement number), а также флаги SYN, ACK и FIN.

Результатом выполнения алгоритма синтеза тестового СТ являются файлы $\langle T_i \rangle_{i=1}^{n_z}$, содержащие пакеты тестового СТ и отражающие осуществляемое через соответствующие СИ ТКО взаимодействие в ССФ ТКО, заданной параметрами модели.

Для подтверждения адекватности разработанной модели был произведен эксперимент, заключающийся в выполнении следующих шагов:

1) Анализ ряда образцов СТ существующих компьютерных сетей, в качестве которых были использованы массивы пакетов, представленные в архиве сети Интернет5, CAIDA6 и MAWI7 и содержащие пакеты штатного взаимодействия компьютерных сетей с использованием протоколов IP-телефонии (SIP и RTP), HTTP, FTP, NetBIOS и DNS, а также различ-

ных реализаций атак типа «отказ в обслуживании» таких как ARP Poisoning, UDP Flood, ICMP Flood и TCP SYN Flood. В результате анализа для каждого из образцов СТ были вычислены значения параметров модели ССФ ТКО.

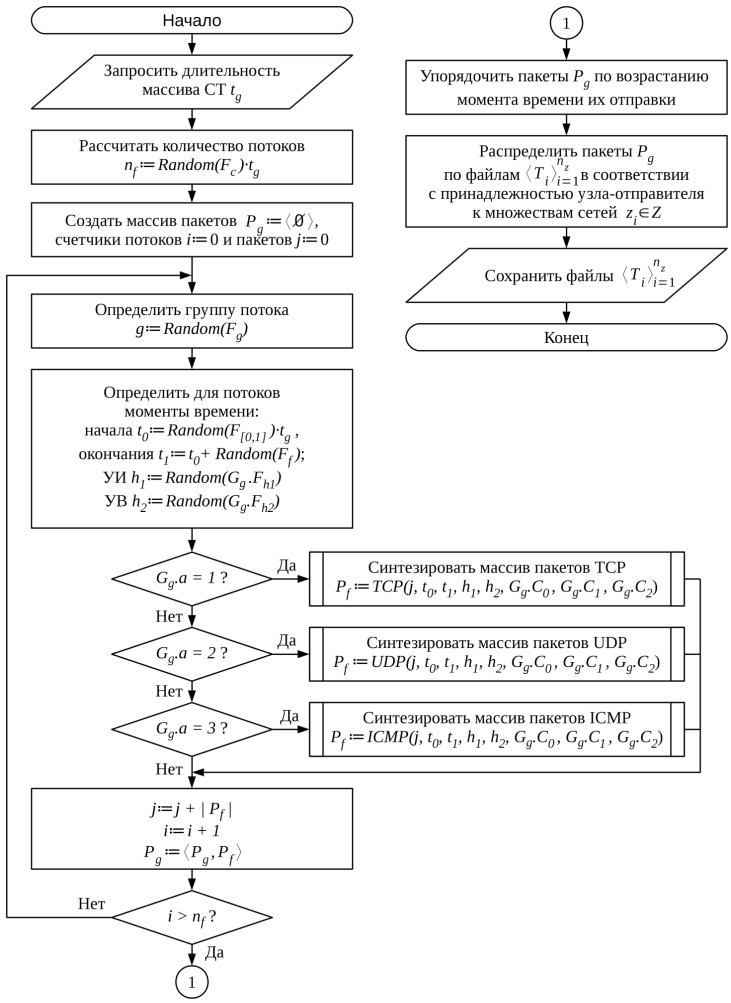

Рис. 1. Блок-схема алгоритма синтеза тестового СТ на основе параметров модели ССФ ТКО

2) Синтез образцов тестового СТ на основе значений параметров модели, вычисленных на предыдущем шаге, с использованием приведенного на рис. 1 алгоритма синтеза тестового СТ.

3) Сопоставление характеристик соответствующих образцов исходного и синтезированного СТ.

Сравнение свойств самоподобия соответствующих образцов СТ компьютерных сетей и синтезированного СТ было проведено в соответствии со схемой, приведенной на рис. 2, путем вычисления двухвыборочного критерия согласия Колмогорова-Смирнова на основе значений интенсивности передачи данных b и межпакетного временного интервала t_p. При размере выборки $n = 20$ образцов СТ были получены следующие максимальные значения статистик: $d_b = 0{,}1$, $d_t = 0{,}15$. Данные статистики соответствуют доверительным интервалам: $p_b = 0{,}999$ и $p_b = 0{,}966$, — что позволяет принять гипотезу о том, что существует статистически достоверная связь между свойствами самоподобия СТ компьютерных сетей и СТ, синтезированного на их основе, на уровне значимости $p < 0{,}04$.

Также в процессе эксперимента были оценены средние значения и дисперсия следующих параметров образцов СТ: количества одновременно взаимодействующих узлов, доли пакетов, генерируемых инициаторами потоков, межпакетных временных интервалов и размеров пакетов. Относительное отклонение данных параметров синтезирован-

ного СТ от параметров соответствующих образцов СТ компьютерных сетей не превысило 0,02.

Результаты экспериментов показали, что представленная модель ССФ ТКО позволяет отразить в синтезируемом с ее применением

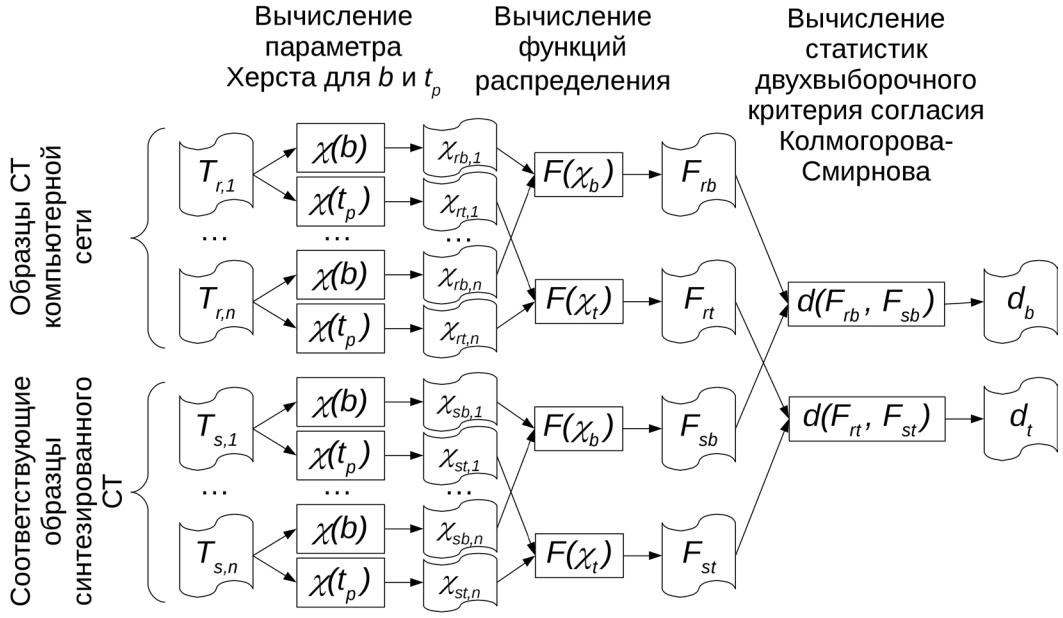

Рис. 2. Схема вычисления статистик двухвыборочного критерия согласия Колмогорова-Смирнова для соответствующих образцов СТ компьютерных сетей и синтезированного СТ

Для оценки способности модели отразить наличие в образцах СТ атакующего воздействия типа «отказ в обслуживании» был произведен их анализ с использованием системы обнаружения атак *Snort*. Все СКА, выявленные системой обнаружения атак в соответствующих образцах исходного и синтезированного СТ, были классифицированы идентично, что подтверждает способность модели отразить в синтезируемом СТ параметры как штатного информационного взаимодействия, так и атакующего воздействия типа «отказ в обслуживании», направленного на ТКО.

тестовом СТ свойство самоподобия, структуру и статистические характеристики трафика заданной сетевой среды, в которой производится эксплуатация образца ТКО, при проведении направленных на него СКА типа «отказ в обслуживании».

Таким образом, разработанная модель позволяет обеспечить адекватность результатов тестирования ТКО, а ее применение в процессе аудита информационной безопасности компьютерных сетей способствует повышению их защищенности от СКА типа «отказ в обслуживании».

Примечания

1. Sridhar S. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis / S. Sridhar. — Essex : School of Computer Science and Electronic Engineering, University of Essex, 2011. — 47 p.

2. Шелухина О.И. Самоподобие и фракталы. Телекоммуникационные приложения / О.И. Шелухина, А.В. Осин, С.М. Смольский. — М. : Физматлит, 2015. — 368 с.

3. Heusse M. Router and switch architecture // Laboratorie d'infomatique de Grenoble. URL: http://lig-membres.imag.fr/heusse/archi_routeur.pdf (дата обращения: 20.06.2017).

4. Вентцель Е. С. Теория вероятностей. — М. : Наука, 1969. — 576 с.

5. The Internet traffic archive // ACM SIGCOMM. URL: http://ita.ee.lbl.gov (дата обращения: 20.06.2017).

6. CAIDA Internet Data. Passive Data Sources // Center for Applied Internet Data Analysis. URL: http://www.caida.org/data/passive (дата обращения: 20.06.2017).

7. MAWI Working Group Traffic Archive // Measurement and Analysis on the Wide Internet Working Group. URL: http://mawi.wide.ad.jp (дата обращения: 20.06.2017).

Алексей Владимирович АГАФОНОВ, аспирант кафедры алгебры и фундаментальной информатики Института естественных наук и математики УрФУ им. первого Президента России Б.Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19, avagaf@gmail.com, (343) 375-95-40.

Alexey AGAFONOV, Postgraduate at the Department of Algebra and Fundamental Informatics, Institute of Natural Sciences and Mathematics, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Russian Federation, Yekaterinburg, Mira str., 19, avagaf@gmail.com, (343) 375-95-40.