Математические структуры и моделирование 2018. № 2(46). С. 125–134

УДК 004.056
DOI: 10.25513/2222-8772.2018.2.125-134

АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПРИМЕНЕНИЯ ЭВОЛЮЦИОННО–ГЕНЕТИЧЕСКОГО ПОДХОДА

Н.И. Синадский
доцент, к.т.н., e-mail: nickis@e1.ru
А.В. Агафонов
ассистент, e-mail: avagaf@gmail.com

Институт радиоэлектроники и информационных технологий УрФУ им. первого Президента России Б.Н. Ельцина, Екатеринбург, Россия

Аннотация. В статье рассмотрен подход к тестированию устойчивости сетевых средств защиты информации к компьютерным атакам типа «отказ в обслуживании» на основе применения аппарата генетических алгоритмов.

Ключевые слова: тестирование, сетевые средства защиты информации, отказ в обслуживании, генетический алгоритм.

Введение

Одной из актуальных угроз информационной безопасности существующих информационно–телекоммуникационных сетей являются компьютерные атаки типа «отказ в обслуживании», направленные как на отдельные узлы данных сетей, так и на их технологическую инфраструктуру.

Объектами атак могут являться в том числе и сетевые средства защиты информации (ССЗИ), такие как межсетевые экраны и системы предотвращения вторжений. Успешная реализация атаки в данных случаях приводит к нарушению или существенному снижению доступности информации, обрабатываемой узлами сетей, что актуализирует задачу тестирования устойчивости ССЗИ от атак указанного типа.

Наиболее широко применяемым методом оценки защищённости оборудования компьютерных сетей от атак типа «отказ в обслуживании» является его натурное тестирование в изолированной сетевой среде с применением синтезированного сетевого трафика (СТ), имитирующего комбинацию СТ штатного информационного взаимодействия узлов компьютерной сети и атакующего воздействия.

Разработанная авторами методика тестирования ССЗИ подразумевает передачу тестового СТ, в процессе которой производится оценка способности тестируемого оборудования обеспечивать заданный требованиями компьютерной

сети уровень доступности информации. Данный уровень может быть описан совокупностью следующих параметров: среднего значения задержки передачи пакетов $\overline{t_d}$, его среднеквадратического отклонения $\sigma(\delta t_p)$, называемого также джиттером, и относительной доли потерь пакетов q, — которые могут быть заданы вектором в пространстве $\Omega = \{\omega\}$, где вектор ω определяется следующим выражением:

$$\omega = \langle \overline{t_d}, \sigma(\delta t_p), q \rangle. \tag{1}$$

Особенностью рассматриваемых сетевых компьютерных атак является то, что при их реализации не задействуется прикладной уровень модели OSI и, в большинстве случаев, применяется СТ, соответствующий спецификациям используемых протоколов передачи данных, параметры которого отличаются от штатного СТ лишь количественно [1].

Поэтому до проведения тестирования ССЗИ нельзя предугадать все возможные сочетания параметров СТ атакующего воздействия, к которому оно оказывается уязвимо.

Современные исследования показали влияние на успешность реализации сетевых компьютерных атак типа «отказ в обслуживании», направленных на ССЗИ, следующих параметров СТ: n_e, n_w, n_z — количества взаимодействующих узлов, сетей и задействованных в процессе взаимодействия сетевых интерфейсов ССЗИ; p_{tcp}, p_{udp}, p_{icmp} — относительных доль потоков TCP, UDP и сеансов взаимодействия ICMP; $\overline{n_f}$, $\overline{t_f}$, $\overline{l_p}$, $\overline{t_p}$, $\overline{p_{h1}}$ — средних значений количества, длительности потоков, размера пакетов, межпакетного временного интервала и относительной доли пакетов, сгенерированных узлами-инициаторами логических соединений; $\sigma(n_f)$, $\sigma(t_f)$, $\sigma(l_p)$, $\sigma(t_p)$, $\sigma(p_{h1})$ — соответствующих им среднеквадратических отклонений.

Таким образом, может быть определено пространство $\Psi = \{\psi\}$ параметров тестового СТ, значимых в задаче оценки защищённости ССЗИ от сетевых компьютерных атак типа «отказ в обслуживании», где вектор ψ определяется следующим выражением:

$$\begin{aligned} \psi \;=\; & \big\langle n_e, n_w, n_z, p_{tcp}, p_{udp}, p_{icmp}, \overline{n_f}, \overline{t_f}, \overline{l_p}, \overline{t_p}, \overline{p_{h1}}, \\ & \sigma(n_f), \sigma(t_f), \sigma(l_p), \sigma(t_p), \sigma(p_{h1}) \big\rangle \end{aligned} \tag{2}$$

Поиск сочетаний параметров СТ атакующего воздействия, к которому ССЗИ оказывается уязвимо, необходимый для обеспечения полноты тестирования, является задачей переборного типа, которая может быть сведена к задаче отыскания экстремума многомерной функции $\psi(\omega)$. Численное решение данного класса задач может быть затруднено в связи с размерностью и видом исследуемой функции, которая в общем случае может быть нелинейной, разрывной, недифференцируемой и многоэкстремальной [2].

Наиболее перспективным методом решения данного класса задач является эволюционно–генетический подход, который используется для построения алгоритмов поиска оптимальных решений, называемых генетическими алгоритмами, на основе моделирования таких механизмов биологической эволюции, как размножение, мутация и отбор особей популяции.

Генетический алгоритм тестирования сетевых средств защиты информации

Блок-схема разработанного генетического алгоритма приведена на рис. 1.

Каждая из особей μ_i популяции $\mu = \{\mu_i\}_{i=1}^{n_\mu}$ представляет собой совокупность значений статистических параметров, на основе которых производится синтез тестового СТ, имеющего заданную структуру. Параметры особи μ_i представляются в процессе работы генетического алгоритма в виде последовательности бит $\chi_i = \langle \chi_{i,j} \rangle_{j=1}^{n_\chi}$, где $\chi_i = \{0, 1\}$, называемой далее хромосомой.

На предварительном этапе работы генетического алгоритма с использованием функции $RandomM(M)$, где M — математическая модель, описывающая структуру параметров особи, производится инициализация параметров особей случайными значениями, на основе которых затем выполняется синтез образцов тестового СТ с заданными характеристиками $\psi_i \in \Psi$.

Образцы синтезированного СТ используются для тестирования ССЗИ, в процессе которого определяется уровень обеспечиваемой ССЗИ доступности информации, $\omega_i \in \Omega$. Данные векторы $\omega = \{\omega_i\}_{i=1}^{n_\mu}$ затем используются для ранжирования популяции по убыванию значений критерия оптимальности γ_i, определяемого для особи μ_i как количество особей популяции, которым соответствуют меньшие значения всех параметров доступности информации, входящих в вектор ω_i:

$$\gamma_i = \left| \bigcap_{i=1}^{3} \{ \mu_k \mid \forall k : \omega_{i,j} > \omega_{k,j} \} \right|. \tag{3}$$

В разработанном генетическом алгоритме размер популяции изменяется на каждом шаге его работы на основе анализа динамики изменения максимальных и средних значений параметров доступности информации по популяции.

В случае если ни один из элементов вектора максимальных значений не увеличил в течение шага работы генетического алгоритма своего значения, то принимается гипотеза о том, что комбинации существующих решений в процессе кроссинговера не показывают большей степени приспособленности, чем существующие, поэтому для увеличения скорости поиска новых решений, не являющихся комбинацией существующих, производится увеличение численности популяции. В случае если ни один из элементов вектора средних значений не увеличил своего значения, то принимается гипотеза о том, что популяцией обнаружен и исследуется новый локальный экстремум функции $\psi(\omega)$, поэтому для увеличения быстродействия генетического алгоритма и давления отбора размер популяции уменьшается.

Шаг изменения размера популяции генетического алгоритма принимается равным трём, так как в соответствии с механизмом скрещивания перенос одной родительской особи в следующее поколение вызывает появление двух дополнительных потомков. Минимальный размер популяции равен шести, так как для процедуры скрещивания необходимы как минимум две особи, каждая из которых генерирует по два потомка.

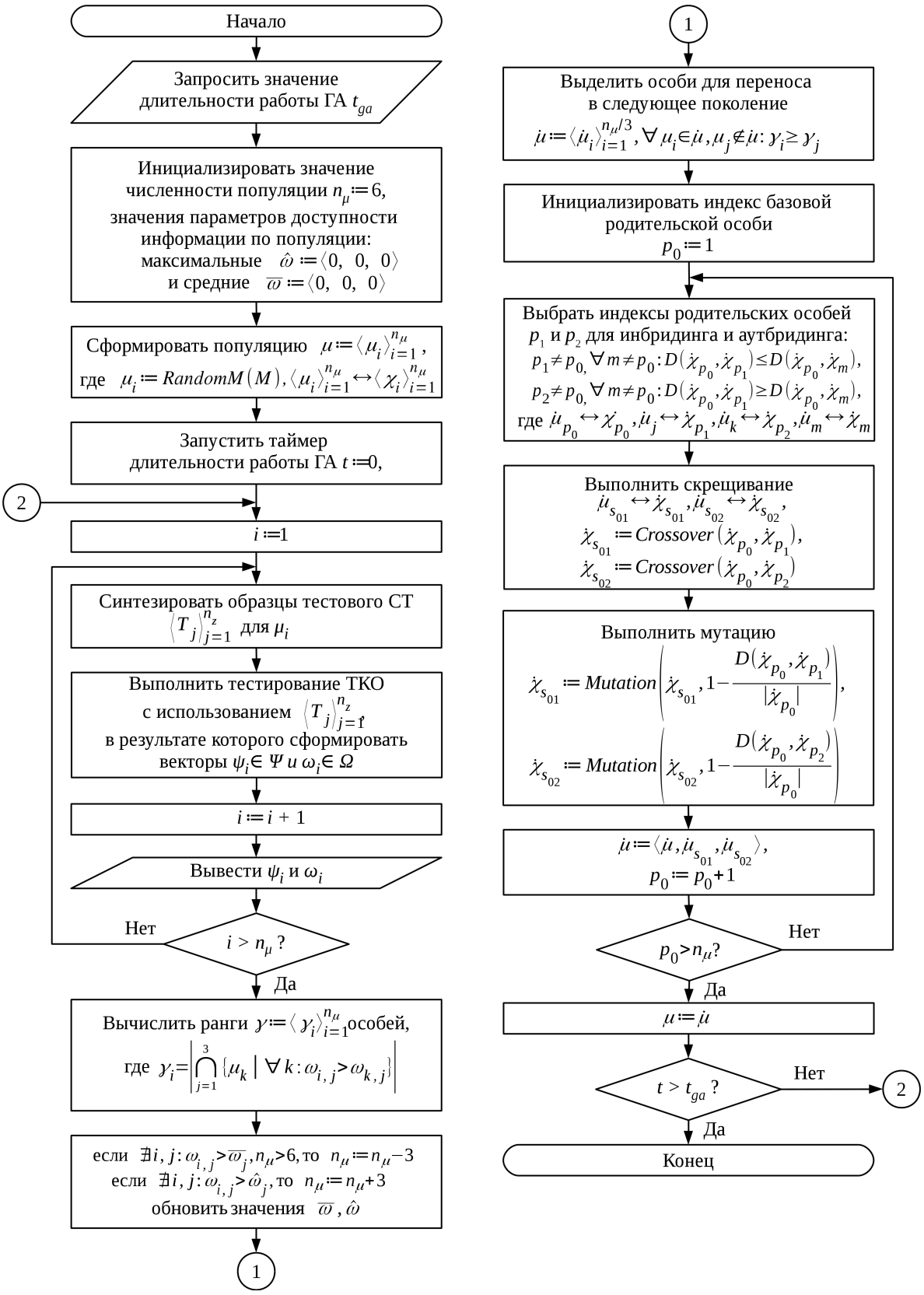

Рис. 1. Блок-схема генетического алгоритма

Для выделения особей, переходящих в следующее поколение в процессе выполнения разработанного генетического алгоритма, используется механизм элитного отбора, заключающийся в построении популяции следующего поколения из имеющих наибольшее значение критерия оптимальности.

В качестве механизма отбора особей для скрещивания используется метод, являющийся комбинацией инбридинга и аутбридинга. Инбридинг заключается в выборе пар особей популяции, имеющих наименьшие различия особей; аутбридинг — в выборе особей, имеющих наибольшие различия, мерой которых является расстояние Хэмминга $D(\chi)$ между их хромосомами.

Подбор особей в родительские пары при инбридинге приводит к скрещиванию особей со сходными параметрами, поэтому данный механизм позволяет сохранить имеющиеся удачные сочетания параметров СТ, производя поиск больших значений функции $\omega(\psi)$ вблизи родительских особей.

Аутбридинг позволяет избежать потери разнообразия исследуемых сочетаний параметров СТ за счёт смешения при скрещивании значительно различающихся хромосом, которые переносятся на следующую итерацию генетического алгоритма.

При выполнении процедуры скрещивания $Crossover(\chi_{p1}, \chi_{p2})$ выполняется двухточечный кроссинговер хромосом родительских особей χ_{p2}, χ_{p2}, заключающийся в случайном выборе двух точек разрыва r_1 и r_2 хромосом.

При этом хромосома дочерней особи χ_c определяется следующим образом:

$$\chi_c = \langle \chi_{c,i} \rangle_{i=1}^{n_\chi}, \text{где } \chi_{c,i} = \begin{cases} \chi_{p1,i}, & \text{если } i \in [r_1, r_2] \\ \chi_{p2,i}, & \text{если } i \notin [r_1, r_2] \end{cases}. \tag{4}$$

Мутация особей выполняется процедурой $Mutation(\chi)$ методом сальтации, заключающимся в выборе в хромосоме особи χ границ $j_0, j_1 \in [1, n_\chi - 1]$, где $j_0 < j_1$, в пределах которых производится замена значений бит хромосомы на противоположные. В результате формируется изменённая хромосома:

$$\dot{\chi} = \langle \dot{\chi}_i \rangle_{i=1}^{n_\chi}, \text{где } \dot{\chi}_i = \begin{cases} \chi_i, & \text{если } i \in [j_0, j_1] \\ \chi_i \oplus 1, & \text{если } i \notin [j_0, j_1] \end{cases}. \tag{5}$$

Мутация особей выполняется лишь для особей, сгенерированных на текущем шаге работы генетического алгоритма, причём вероятность мутации p_{mut} определяется в соответствии с расстоянием Хэмминга между хромосомами её родительских особей следующим образом:

$$p_{mut} = 1 - \frac{D(\dot{\chi}_{p1}, \dot{\chi}_{p2})}{|\dot{\chi}_{p1}|}. \tag{6}$$

Данный механизм позволяет избежать сходимости популяции к локальным экстремумам критерия оптимальности решения за счёт высокой вероятности мутации для особей, имеющих слабо отличающиеся родительские хромосомы, и сохранить при этом наилучшие решения за счёт отсутствия мутации особей, переходящих из поколения в поколение.

На очередную итерацию генетического алгоритма переносятся лучшие особи текущей итерации, соответствующие наибольшим значениям $\omega(\psi)$, и их потомки в пропорции один к двум.

Критерием остановки генетического алгоритма является истечение заданного пользователем временного интервала.

Результатом работы генетического алгоритма является база данных, содержащая множество точек $\rho = \{\rho_i \mid \rho_i \in \Psi \times \Omega\}$, где $\rho_i = \langle \psi_i, \omega_i \rangle$, $\psi_i \in \Psi$, $\omega_i \in \Omega$, отражающих соответствие параметров СТ, обрабатываемого ССЗИ, обеспечиваемой им доступности информации. Наихудшие обнаруженные значения параметров доступности информации позволяют определять способность тестируемого ССЗИ удовлетворять требованиям, предъявляемым к компонентам защищаемой компьютерной сети.

Оценка надёжности генетического алгоритма

Разработанный генетический алгоритм предназначен для решения задачи поиска множества экстремумов неизвестной функции $\omega(\psi)$. Поэтому под его надёжностью подразумевается способность к обнаружению данных экстремумов в течение заданного ограниченного интервала времени.

Исследование надёжности было выполнено в соответствии со схемой, представленной на рис. 2, где МГА — модуль, реализующий разработанный генетический алгоритм; МИТ — модуль имитации тестирования ССЗИ с использованием СТ, обладающего заданными параметрами $\psi \in \Psi$, тестовой функции ТФ $\omega(\psi)$, отражающей зависимость вектора параметров доступности информации от параметров СТ; МАРТ — модуль анализа результатов тестирования.

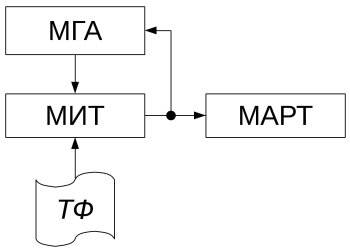

Рис. 2. Структура стенда для тестирования надежности генетического алгоритма

Каждый из компонентов тестовой функции $\omega(\psi)$ содержит шумовую составляющую, затрудняющую поиск экстремумов, и информационную, содержащую искомые экстремумы. В качестве данных составляющих используются функции, широко применяемые при исследовании надёжности генетического алгоритма [3], критерием выбора которых является отсутствие ограничений по размерности вектора их аргументов для возможности представления многомерного пространства параметров. В качестве шумовой составляющей использована функция Растригина, особенностью которой является большое количество локальных экстремумов. В качестве информационной составляющей использована функция Михалевича, особенностью которой является наличие большого

количества локальных экстремумов и одного — глобального, которые занимают относительно небольшую часть области определения функции, что повышает сложность решения задачи поиска.

В результате выполнения серии из 100 запусков генетического алгоритма при выбранных случайным образом значениях коэффициентов тестовой функции были получены зависимости средних, минимальных и максимальных значений доли выявленных экстремумов. Графики, отражающие данные зависимости, приведены на рис. 3.

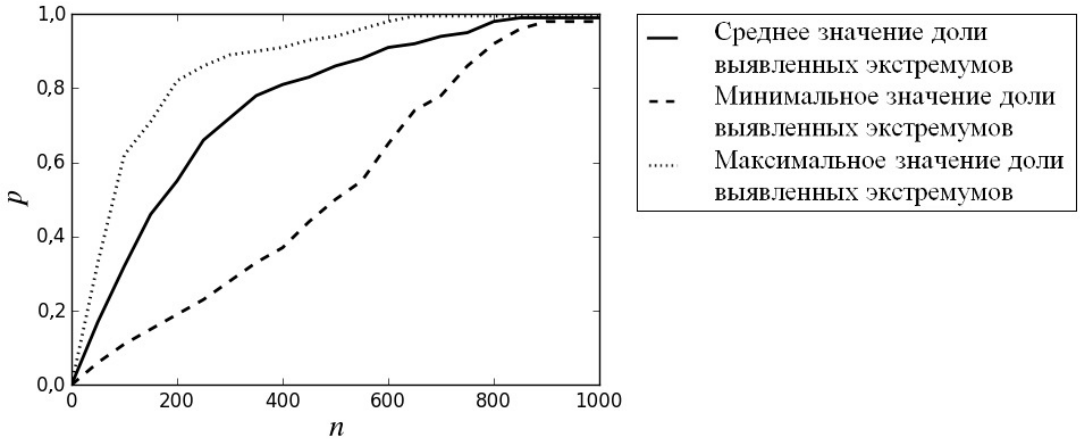

Рис. 3. Зависимость доли выявленных экстремумов от количества исследованных генетическим алгоритмом точек тестовой функции

Результаты эксперимента показали, что разработанный генетический алгоритм при количестве исследованных точек тестовой функции не менее 850 позволяет выявить не менее 98 % её локальных и глобальных экстремумов. В рамках методики IETF RFC 2544 [4], широко применяемой на сегодняшний день для тестирования различного оборудования, используемого в компьютерных сетях, устанавливается минимальная длительность генерации образца СТ, равная 120 с. При использовании указанной длительности исследование приведённого количества точек занимает менее 30 часов, что может служить подтверждением надёжности генетического алгоритма и его способности к решению задачи выявления экстремумов заданной функции в течение ограниченного интервала времени.

Разработанный генетический алгоритм позволяет автоматизировать процесс поиска уязвимостей ССЗИ к сетевым компьютерным атакам типа «отказ в обслуживании» путём подбора таких сочетаний параметров СТ атакующего воздействия, при которых ССЗИ оказывается неспособно обеспечить необходимый уровень доступности информации, обрабатываемой в компьютерной сети. При этом, в отличие от применяемых на сегодняшний день методик автоматизации тестирования (в частности, RFC 2544), предложенный генетический алгоритм позволяет решать данную задачу при большой размерности пространства поиска и позволяет учесть все известные параметры СТ, оказывающие влияние

на устойчивость ССЗИ к рассматриваемому типа атак.

Результаты практического применения генетического алгоритма

Для апробации предложенного генетического алгоритма разработан экспериментальный стенд, с помощью которого было произведено тестирование ряда образцов ССЗИ.

Результатом тестирования образца ССЗИ на данном стенде является множество критических областей пространства параметров сетевого трафика Ψ. Каждая из указанных областей определяет параметры сетевого трафика атаки типа «отказ в обслуживании», к которой уязвимо ССЗИ. Уязвимость ССЗИ выражается в том, что значение по крайней мере одного из параметров доступности информации $\omega \in \Omega$, обеспечиваемой им при обработке сетевого трафика атакующего воздействия, выходит за граничные значения, допустимые для данной компьютерной сети.

Критерием выявления критических областей выступило несоответствие требованиям стандарта МСЭ-Т Y.1541 [5] к сетям нулевого класса, предназначенным для исполнения приложений реального времени, которые накладывают следующие требования к доступности информации: относительная доля потерь пакетов q должна быть менее 0,001, джиттер $\sigma(\delta t_p)$ — менее 50 мс, а средняя задержка передачи пакетов $\overline{t_d}$ — менее 100 мс.

В частности, было выполнено тестирование фильтрующего маршрутизатора Cisco 2811, широко применяемого в сетях средних и крупных предприятий в качестве межсетевого экрана. В соответствии с документацией устройство имеет следующие технические характеристики:

- пропускная способность 61 Мбит/с;
- предельная интенсивность пересылки — 120000 пакетов/с;
- объём оперативной памяти 256 Мбайт.

Результаты тестирования маршрутизатора приведены на лепестковой диаграмме (рис. 4).

В результате тестирования были выявлены параметры сетевой компьютерной атаки типа «отказ в обслуживании», характеризующейся потерями пакетов $q \in [0{,}03, 0{,}06]$ и обусловленной достижением образцом ССЗИ предельного значения интенсивности передачи данных $I_d \in [61, 78]$ Мбит/с, соответствующего приведённому в документации образца.

Также была выявлена критическая область, соответствующая ранее неизвестной компьютерной атаке.

Данная критическая область показывает, что высокие значения потерь пакетов $q \in [0{,}05, 0{,}06]$ и джиттера $\sigma(\delta t_p) \in [51, 59]$ мс возникают при обработке образцом ССЗИ сетевого трафика относительно низкой интенсивности $I_d \in [51, 59]$ Мбит/с, где наблюдаются относительно высокие значения вариативности межпакетных временных интервалов $\sigma(t_p) \in [2{,}2, 2{,}9]$ мкс и средней интенсивности генерации потоков $\overline{n_f} \in [680, 815]$ потоков/с.

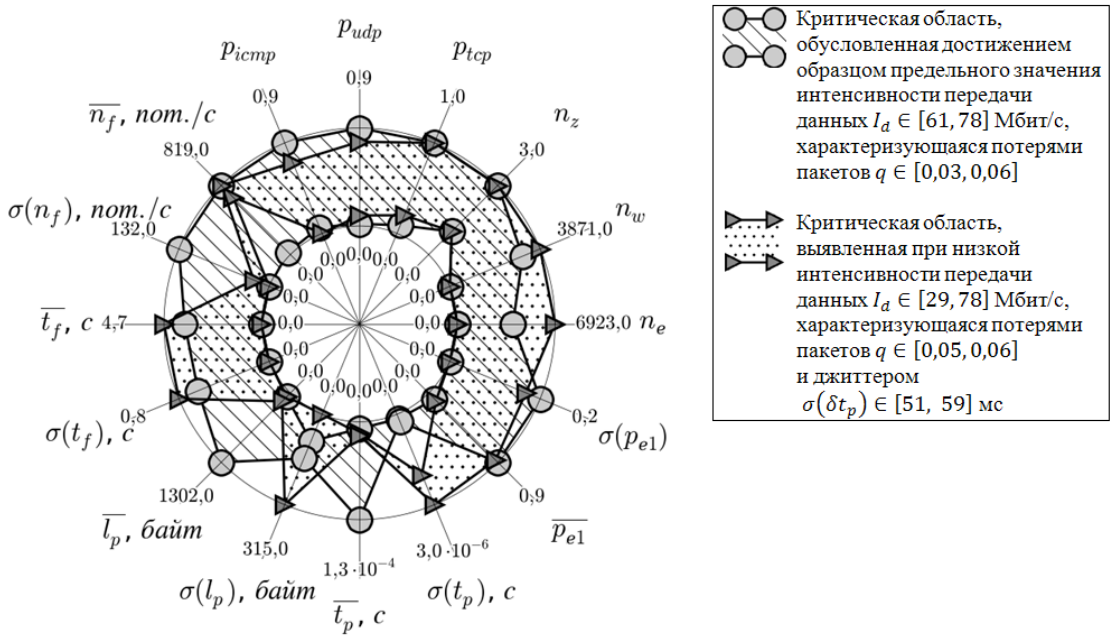

Рис. 4. Результаты тестирования фильтрующего маршрутизатора Cisco 2811

Выводы

Принцип работы разработанного генетического алгоритма тестирования ССЗИ основан на поиске экстремумов многомерной функции, отражающей зависимость между параметрами СТ, обрабатываемого ССЗИ, и обеспечиваемой им доступности информации. Данный поиск производится путём многократного тестирования ССЗИ с использованием различных образцов синтезированного СТ.

Результаты работы генетического алгоритма позволяют определить наихудшие показатели доступности информации, которые тестируемое ССЗИ способно обеспечить в процессе проведения сетевых компьютерных атак типа «отказ в обслуживании», что позволяет производить обоснованный выбор образцов ССЗИ, наиболее устойчивых к данному типу атак, и, таким образом, способствует обеспечению информационной безопасности информационно–телекоммуникационных систем и сетей.

Литература

1. Sridhar S. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis. Essex : School of Computer Science and Electronic Engineering, University of Essex, 2011. 47 p.
2. Батищев Д.И., Неймарк Е.А., Старостин Н.В. Применение генетических алгоритмов к решению задач дискретной оптимизации. Нижний Новгород : изд-во ННГУ, 2007. 88 с.

3. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы; пер. с польск. И.Д. Рудинского. М. : Горячая линия–Телеком, 2006. 452 с.
4. McQuaid S., Bradner J. IETF RFC 2544: Benchmarking methodology for network interconnect devices. URL: `http://www.ietf.org/rfc/rfc2544.txt` (дата обращения: 25.11.2017).
5. ITU-T Y.1541: Network performance objectives for IP-based services. URL: `https://www.itu.int/rec/T-REC-Y.1541-201112-I` (дата обращения: 20.08.2017).

TESTING NETWORK SECURITY DEVICES AUTOMATION USING EVOLUTIONARY-GENETIC APPROACH

N.I. Sinadsky
Ph.D. (Eng.), Associate Professor, e-mail: nickis@e1.ru
A.V. Agafonov
Instructor, e-mail: avagaf@gmail.com

Institute of Radioelectronics and Information Technologies, Ural Federal University n.a. first President of Russia B.N. Yeltsin, Yekaterinburg, Russia

Abstract. The article describes approach for automation of testing the immunity of network security devices against denial of service attacks using genetic algorithms.

Keywords: testing, network security devices, denial of service, genetic algorithm.

Дата поступления в редакцию: 20.04.2018