УДК 004.056 + 621.391 + 004.7.056 Вестник УрФО № 2(24) / 2017, с. 4–8

Агафонов А. В., Синадский Н. И.

ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ ОТ СЕТЕВЫХ КОМПЬЮТЕРНЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» С ПРИМЕНЕНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА

В статье рассмотрен генетический алгоритм, предназначенный для автоматизации тестирования защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением синтезированного сетевого трафика.

Ключевые слова: *тестирование, телекоммуникационное оборудование, отказ в обслуживании, генетический алгоритм.*

Agafonov, Sinadsky N.

TESTING THE IMMUNITY OF TELECOMMUNICATION EQUIPMENT AGAINST DENIAL OF SERVICE NETWORK ATTACKS USING THE GENENTIC ALGORITHM

The article describes the genetic algorithm, intended for automation of testing the immunity of telecommunication equipment against denial of service network attacks using synthesized network traffic

Keywords: *testing, telecommunication equipment, denial of service, genetic algorithm.*

В условиях построения в Российской Федерации информационного общества и формирования глобального информационного пространства подавляющее большинство систем принятия решений и управления в ключевых областях экономики и государственного управления создается с использованием современных информационных технологий. Вследствие этого возрастает важность обеспечения защищенности существующих и проектируемых информационно-телекоммуникационных систем и сетей (ИТСиС) от нарастающих угроз информационного характера, одной из которых являются сетевые компьютерные атаки (СКА) типа «отказ в обслуживании».

Объектом атак данного типа могут являться как отдельные узлы защищаемых ИТСиС, так и обеспечивающее их взаимодействие телекоммуникационное оборудование (ТКО), такое как коммутаторы и маршрутизаторы. Успешная реализация атак на ТКО может привести к одновременному нарушению штатного информационного взаимодействия множества узлов и нанести значительный ущерб. В связи с этим, тестирование защищенности ТКО от СКА типа «отказ в обслуживании» является важным этапом аудита информационной безопасности ИТСиС.

Наиболее широко применяемым методом оценки защищенности ТКО 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. При тестировании осуществляется пересылка тестового СТ с использованием ТКО, в процессе которой производится оценка его способности обеспечить 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 $\sigma(t_d)$, называемого также джиттером, и относительной доли потерь пакетов q, — которые могут быть заданы вектором в пространстве $\Omega = \{\omega\}$, где вектор ω определяется следующим выражением: $\omega = \{\langle \overline{t_d}, \sigma(t_d), q \rangle\}$.

Особенностью рассматриваемых СКА 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 ТКО нельзя предугадать все возможные сочетания параметров СТ атакующего воздействия, к которому оно оказывается уязвимо.

Современные исследования показали влияние на успешность реализации СКА типа «отказ в обслуживании», направленных на ТКО, следующих параметров СТ: n_h, n_w, n_z — количества взаимодействующих узлов, сетей и задействованных в процессе взаимодействия сетевых интерфейсов ТКО; 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 сетевого трафика, значимых в задаче оценки защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании», где вектор ψ определяется следующим выражением:

$$\psi = \{\langle n_h, n_w, n_z, p_{tcp}, p_{udp}, p_{icmp}, \overline{n_f}, \overline{t_f}, \overline{l_p}, \overline{t_p}, \overline{p_{h1}}, \sigma(n_f), \sigma(t_f), \sigma(l_p), \sigma(t_p), \sigma(p_{h1}) \rangle\}.$$

Поиск сочетаний параметров СТ атакующего воздействия, к которому ТКО оказывается уязвимо, необходимый для обеспечения полноты тестирования, является задачей переборного типа, которая может быть сведена к задаче отыскания экстремума многомерной функции $\omega(\psi)$. Численное решение данного класса задач может быть затрудненно 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 (ГА), на основе моделирования таких механизмов биологической эволюции, как размножение, мутация и отбор особей популяции.

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 ГА в виде последовательности n_χ бит $\chi_i = \langle \chi_{i,j} \rangle_{j=1}^{n_\chi}$, где $\chi_{i,j} \in \{0,1\}$, называемой далее хромосомой.

На предварительном этапе работы ГА 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 ТКО, в процессе которого определяется уровень обеспечиваемой ТКО доступности информации, $\omega_i \in \Omega$.

Данные векторы $\{\omega_i\}_{i=1}^{n_\mu}$ 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: $\gamma_i = \left| \bigcap_{j=1}^{3} \{\mu_k \mid \forall k : \omega_{i,j} > \omega_{k,j}\} \right|$.

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 $\overline{\omega}$ не увеличил своего значения, то принимается гипотеза о том, что популяцией обнаружен и исследует-

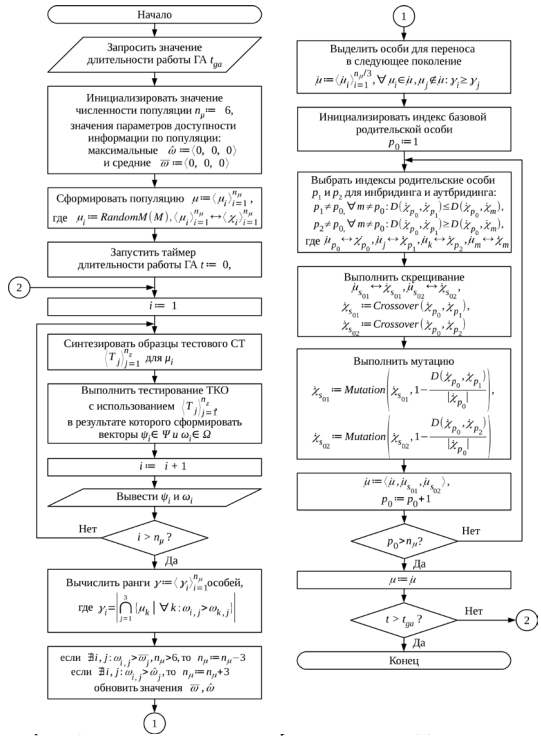

Рис. 1. Блок-схема реализованного генетического алгоритма

щийся 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 счет смешения при скрещивании сильно различающихся хромосом, которые переносятся на следующую итерацию ГА.

При выполнении процедуры скрещивания $Crossover(\chi_{p1}, \chi_{p2})$ выполняется двухточечный кроссинговер хромосом родительских особей χ_{p1}, 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: $\chi_c = \langle \chi_{c,i} \rangle_{i=1}^{n_\chi}$, где $\chi_{c,i} = \begin{cases} \chi_{p1,i}, & \text{если } i \notin [r_1, r_2] \\ \chi_{p2,i}, & \text{если } i \in [r_1, r_2] \end{cases}$.

Мутация особей выполняется процеду-

рой $Mutation$ методом сальтации, заключающимся в выборе в хромосоме особи χ, границ $j_0, j_1 \in \lfloor 1, n_\chi - 1 \rfloor$, где $j_0 < j_1$, в пределах которых производится замена значений бит хромосомы на противоположные. В результате формируется измененная хромосома $\dot{\chi}$: $\dot{\chi} = \langle \dot{\chi}_i \rangle_{i=1}^{n_\chi}$, где $\dot{\chi}_i = \begin{cases} \chi_i, & \text{если } i \notin [j_0, j_1] \\ \chi_i \oplus 1, & \text{если } i \in [j_0, j_1] \end{cases}$.

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

$$p_{mut} = 1 - \frac{D(\dot{\chi}_{p0}, \dot{\chi}_{p1})}{|\dot{\chi}_{p0}|}.$$

Данный механизм позволяет избежать сходимости популяции к локальным экстремумам критерия оптимальности решения за счет высокой вероятности мутации для особей, имеющих слабо отличающиеся родительские особи, и сохранить при этом наилучшие решения за счет 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.

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

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

Каждый из компонентов тестовой функции $\omega(\psi)$ содержит шумовую составляющую, затрудняющую поиск экстремумов, и

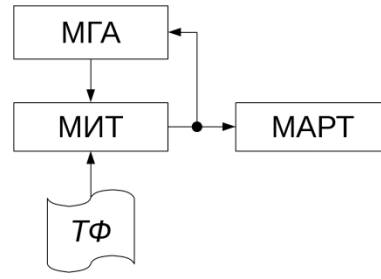

Рис. 2. Структура стенда для тестирования надежности ГА.

информационную, содержащую искомые экстремумы. В качестве данных составляющих используются функции, широко используемые при исследовании надежности ГА3, 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 ГА при различных значениях коэффициентов тестовой функции были получены зависимости средних, минимальных и максимальных значений доли выявленных экстремумов. Графики, отражающие данные зависимости, приведены на рис. 3.

Результаты эксперимента показали, что разработанный генетический алгоритм при количестве исследованных точек тестовой функции не менее 850 позволяет выявить не менее 98% ее локальных и глобальных экстремумов. В рамках широко применяемой на сегодняшний день методики IETF RFC 25444 устанавливается минимальная длительность сеанса тестирования, равная 120 секундам. При использовании указанной длительности исследование приведенного количества точек занимает менее 30 часов, что может служить подтверждением надежности генетического алгоритма и его способности к решению задачи выявления экстремумов заданной функции в течение ограниченного интервала времени.

Разработанный ГА позволяет автоматизи-

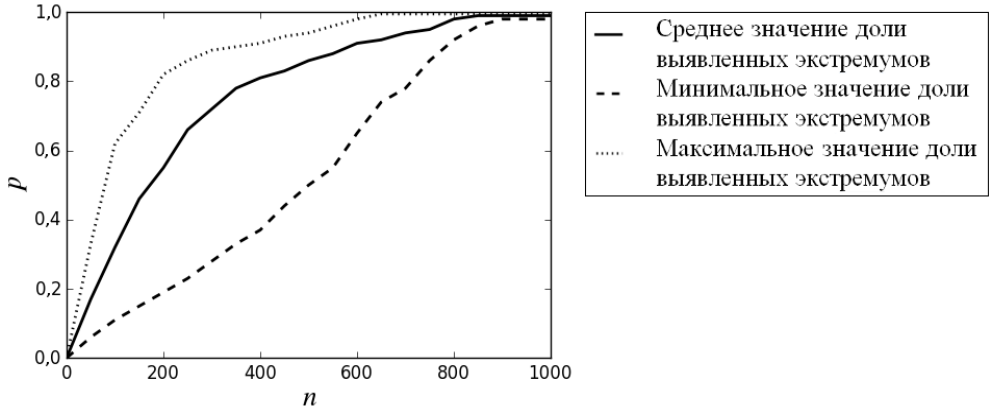

Рис. 3. Зависимость доли выявленных экстремумов p от количества исследованных генетическим алгоритмом точек тестовой функции n

ровать процесс поиска уязвимостей ТКО к СКА типа «отказ в обслуживании» путем подбора таких сочетаний параметров СТ атакующего воздействия, при которых ТКО оказывается неспособно обеспечить необходимый уровень доступности информации, обрабатываемой в ИТСиС. При этом, в отличие от применяемых на сегодняшний день методик автоматизации тестирования (в частности, RFC 2544), предложенный ГА позволяет решать данную задачу при большой размерности пространства поиска и позволяет учесть все известные параметры СТ, оказывающие влияние на устойчивость ТКО к рассматриваемому типа атак. Таким образом, применение разработанного ГА для тестирования ТКО способствует повышению достоверности результатов аудита информационной безопасности ИТСиС.

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] Батищев Д.И. Применение генетических алгоритмов к решению задач дискретной оптимизации [Текст] / Д.И. Батищев, Е.А. Неймарк, Н.В. Старостин. — Нижний Новгород : изд-во ННГУ, 2007. — 88 с.

[3] Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский ; пер. с польск. И.Д. Рудинского [Текст]. — 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: 25.06.2017).

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.

Николай Игоревич СИНАДСКИЙ, к.т.н., доцент, доцент кафедры алгебры и фундаментальной информатики Института естественных наук и математики УрФУ им. первого Президента России Б.Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19, nickis@e1.ru, (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.

Nikolay SINADSKY, Candidate of Engineering Sciences, Docent, Associate Professor at the Department of Algebra and Fundamental Informatics, Institute of of Natural Sciences and Mathematics, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Russian Federation, Yekaterinburg, Mira str., 19, nickis@e1.ru, (343) 375-95-40.