УДК 004.75 DOI:10.31854/1813-324X-2020-6-2-113-120

Модель синтеза распределенных атакующих элементов в компьютерной сети

М.Ю. Петров[1], **Р.Р. Фаткиева**[1*]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, 199198, Российская Федерация
*Адрес для переписки: rikki2@yandex.ru

Информация о статье
Поступила в редакцию 28.04.2020
Принята к публикации 25.06.2020

Ссылка для цитирования: Петров М.Ю., Фаткиева Р.Р. Модель синтеза распределенных атакующих элементов в компьютерной сети // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 113–120. DOI:10.31854/1813-324X-2020-6-2-113-120

Аннотация: *Приведен подход к прогнозированию развития атак на сетевые ресурсы с использованием распределенных атакующих средств. Представлены отличительные особенности сценариев атак. Описана модель функционирования сети с распределенными атакующими элементами. Показано, что моделирование динамики с применением энтропийного подхода к оценке устойчивости не дает возможности идентифицировать наличие атаки. Предложен способ обнаружения координационного центра, осуществляющего атаку.*

Ключевые слова: *распределенные атаки, ботнет сети, марковские процессы, системы обнаружения вторжений, моделирование атак.*

Введение

От эффективности функционирования современных компьютерных сетей во многом зависит успешность деятельности практически во всех сферах общества. С каждым годом происходит увеличение пространственно-временной конфигурации сценариев атак, особенностями которых являются наличие мощности атаки, позволяющей осуществить либо массированный удар на атакуемый ресурс (например, Ddos-атака), либо осуществить скрытое воздействие для проникновения в заданный объект. При этом процесс автоматизации сценариев атаки позволяет осуществить перебор уязвимых мест для нахождения точек входа в атакуемую систему с возможностью ее изменения при «залатывании бреши» средствами защиты информации. Другой специфической особенностью является децентрализация систем управления атаками, как ответный механизм на возможность выявления источника атаки. Примером является дополнение Интернета реализацией второго поколения так называемой луковой маршрутизации. Это приводит к сбалансированности механизмов атаки и распределению атакующих элементов в ходе ее выполнения. Автоматизация выполнения атаки позволяет осуществить интеграцию сценариев атаки из заданного заранее множества. Это дает временные преимущества при реализации быстрой реконфигурации и адаптации механизмов атаки при выявлении ее системами защиты информации. В этих условиях средства защиты не успевают осуществлять выявление атак при динамическом изменении этапов атаки.

Ущерб от нарушения функционирования вычислительных сетей в результате таких деструктивных воздействий со стороны распределенных атак может исчисляться в миллионах и миллиардах рублей. Проблема обостряется и тем, что в динамически изменяющихся условиях сетевой активности сценарии взаимодействия могут молниеносно переходить в противоборство. Это требует введения систем мониторинга за состоянием компьютерных сетей и прогнозирования их поведения. Однако трудность мониторинга и анализа внутреннего состояния обусловлена огромным многообразием вероятностных состояний. В этих условиях возникает противоречие как в выборе набора показателей для прогнозирования, так и в моделях функционирования компьютерных сетей. Особенно остро этот вопрос стоит при формировании показателей, отражающих взаимодействие систем, с использованием компьютерных сетей, при интеграции ресурсов для достижения поставленных целей. Существующие на рынке системы мониторинга и управления не позволяют учитывать динамику изменений страте-

гий при сетевом взаимодействии, что может привести к снижению устойчивости при отсутствии их согласованности. Таким образом, можно сделать вывод о том, что проблема выявления распределенных атакующих элементов весьма актуальна.

В настоящее время для математического и программного обеспечения мониторинга, защиты и восстановления вычислительных сетей от деструктивных воздействий преимущественно используются модели этих сетей и протекающих в них процессов, а также модели самих процессов мониторинга, защиты и самовосстановления, разработанные без учета структурной динамики сети.

В работе [1] рассмотрена классификация ботнет-сети. В зависимости от топологии распределения атакующих элементов определены признаки, позволяющие идентифицировать DDos-атаку. Спроектированная нейронная сеть идентифицирует аномальное поведение на базе рассмотренных признаков и позволяет обнаружить автономное распределенное вредоносное программное обеспечение, синхронизируемое с помощью команд злоумышленника, передаваемых по сетям общего пользования. В работах [2–4] анализируется структура ботнет-сетей и оценка загрузки каналов передачи информации для расчета предельной пропускной способности. В [5–7] представлены методы обнаружения ботнетов на основе многоагентного подхода, позволяющие обнаруживать распределенные сетевые атаки независимо от протокола передачи данных и организационной структуры, используя кластерный анализ сетевого трафика. В работе [8] сформирована модель оценки рисков сетевой безопасности на основе мультиагентного подхода построения графов атак. В исследованиях [9–14] проведено математическое моделирование распределенных атак на основе марковских процессов. В работе [12] представлены методы, позволяющие определять вероятностные и временные характеристики, описывающие состояния процесса функционирования сети при различных стратегиях установления и поддержания параметров соединений взаимодействующими сторонами, что позволяет оценивать состояние взаимодействия сторон. В [13] представлен метод, основанный на доверии к трафику, с оценкой валидности всех узлов и трафика циркулирующего в сети.

Однако в перечисленных работах не рассматриваются вопросы оценки влияния успешности атаки при использовании распределенных атакующих средств, оценки устойчивости проведения процесса атаки при их использовании, а также вопросы оптимизации средств защиты на устройствах сети при борьбе с распределенными атакующими элементами. В описанных условиях быстрой мутации и разнообразии сетевых атак, необходимости их своевременного обнаружения и предотвращения возникает потребность введения новых механизмов адаптации существующих средств защиты информации в динамически изменяющихся условиях распределенных атак.

Постановка задачи

Рассмотрим постановку задачи на примере многоагентной сети с распределенными атакующими элементами, осуществляющей сетевую атаку. В обобщенном виде процесс доступа к вычислительному ресурсу, представлен в виде графа состояний [14].

В этом случае модель функционирования сети можно представить в виде:

$$F = (H, S, Q, M, Z), \quad (1)$$

где H– множество устройств в сети; S – структурная топология сети; Q– множество состояний при функционировании сети; M– модель нарушителя; Z– множество средств защиты.

Тогда с учетом (1) модель нарушителя, представленная атакующими элементами, осуществляющими сетевую атаку может быть сформирована в виде:

$$H_{\text{attack}} = (Alg, El, S, B, T), \quad (2)$$

где H_{attack} – модель с атакующими элементами; Alg – деструктивный алгоритм, выполняемый атакующим элементом; El – структурно-функциональные элементы, на которых осуществляется алгоритм выполнения, расположенные на S – структурной топологии сети; B – база знаний атакующего элемента; T – время выполнения алгоритма.

Так как одними из главных характеристик успешности атаки является минимизация времени ее выполнения и поиск оптимальной конфигурации распределенных атакующих элементов, расположенных на элементах структурной топологии сети, то для построения оптимальных механизмов защиты от подобных атак требуется разработать подход, позволяющий найти оптимальную конфигурацию распределенных атакующих элементов. Это позволит осуществить анализ наиболее уязвимых элементов сети и оптимизировать построение системы защиты с учетом распределенных атакующих элементов и мер противодействия представленным атакам.

Модель функционирования сети с распределенными атакующими элементами

Рассмотрим модель функционирования сети (1). Для успешности передачи информации по сети необходимо рассмотреть вероятности воздействия распределенных атакующих элементов на функционирование сети. Воздействие атакующих элементов на элементы сети и потеря качества функционирования последними могут происходить в любые случайные моменты времени. Процесс перехода из состояния в состояние при воздействии распределенных атакующих элементов

на него может быть представлен в виде дискретного марковского процесса. В этом случае для малых интервалов времени Δt вероятности перехода имеют вид:

$$p_{ii}(t, t+\Delta t) = P\{Q(t+\Delta t) = Q(t+\Delta) = Q_i | Q(t) = Q_i\} = \\ = 1 - \lambda_{ii}(t) \cdot \Delta t + 0(\Delta t),$$

$$p_{ij}(t, t+\Delta t) = P\{Q(t+\Delta t) = Q_i\} | Q(t) = Q_i\} \\ = \lambda_{ij}(t) \cdot \Delta t + 0(\Delta t), i \neq j,$$

где $\lambda_{ij}(t)$ – интенсивность перехода, характеризующая число переходов из состояния Q_i в состояние Q_j в единицу времени.

Так как вероятности перехода из одного состояния в другое неотрицательны, и для них должно выполняться условие нормировки, то:

$$\lambda_{ii}(t) = \sum_{\substack{i \neq j \\ j=1}}^{G} \lambda_{ij}(t) \gg 0, \qquad \lambda_{ij}(t) \leq 0. \qquad (3)$$

Переходные вероятности p_{ij} для любого момента времени t удовлетворяют системе линейных дифференциальных уравнений:

$$\frac{d}{dt} p_{ij}(t_0, t) = \sum_{g=1}^{G} \lambda_{gj}(t) p_{ig}(t_0, t), (i, j = \overline{1, G}), \quad (4)$$

где интенсивности переходов определяются соотношениями (3). Решение системы уравнений (4) осуществляется при начальных условиях:

$$p_{ij}(t_0, t) = \delta_{ij} = \begin{cases} 1, & \text{при } i = j \\ 0, & \text{при } i \neq j \end{cases}. \qquad (5)$$

Если для дискретного марковского процесса заданы вероятности состояний $p_{ij}(t_0)$, $j = \overline{1, G}$, в начальный момент времени, то вероятности состояний в момент времени t равны:

$$p_j(t + \Delta t) = \sum_{i=1}^{G} p_i(t) p_{ij}(t, t + \Delta t). \qquad (6)$$

По известным интенсивностям переходов (3) вероятности состояний определяются согласно системе дифференциальных уравнений (4). Так как, для однородного дискретного марковского процесса интенсивности перехода не зависят от времени, то условные вероятности перехода в случае однородного дискретного марковского процесса зависят только от разности $\tau = t - t_0$, т. е. $p_{ij}(t_o, t) = p_{ij}(\tau)$. Поэтому система уравнений превращается в систему обыкновенных дифференциальных уравнений:

$$\frac{d}{dt} p_{ij}(\tau) = \sum_{g=1}^{G} \lambda_{gj}(t) p_{ig}(t), \ (g, i, j = \overline{1, G}) \qquad (7)$$

Решение системы дифференциальных уравнений (7) относительно полученных интенсивностей перехода и начальных состояний (3, 5) для различных наборов значений позволяет осуществить построение множества вариантов расположения распределенных атакующих элементов на сети и множество временных интервалов выполнения целевой функции для каждого варианта. Это, в свою очередь, позволяет определить наилучший вариант построения структуры атакующих элементов, дает возможность осуществить синтез распределенных агентов на сетевых элементах.

Минимизация последствий выявления атаки возможна через математическое ожидание выявления агента защищаемыми элементами сети:

$$M_0 = \sum_{i=0}^{N} \gamma_i P_i(j),$$

где $P_j(j)$ – вероятность выявления системами безопасности на каждом элементе, при j-ом методе защиты; $i = \overline{1, N}$ – количество представленных в системе элементов; γ_i – значение ущерба от нарушения на i-ом элементе.

Данный подход позволяет синтезировать не просто результативные, а оптимальные для сложившихся ситуаций модели распределенных атакующих элементов. Оперативное перестроение адекватных текущим ситуациям моделей за счет изменения расположения структурно-функциональных элементов и времени выполнения деструктивного алгоритма позволяет обеспечить гибкость и увеличить сложность решения задач прогнозирования поведения этих сетей и осложнить задачу обнаружения, с учетом расположения средств защиты информации. С другой стороны, применение подобного подхода позволяет лучше рассмотреть возможное поведение деструктивных алгоритмов на заданной структурной топологии сети, с учетом времени выполнения атаки и сформировать необходимый для противодействия комплекс целесообразных мероприятий защиты, а также повысить эффективность этих мероприятий на уже имеющемся наборе.

Разработка оптимальной конфигурации многоагентной распределенной сети

Рассмотрим моделирование на примере атаки-исследования сети. Процесс атаки представлен в виде граф-схемы (рисунок 1), характеризуется наличием множества агентов, внедренных на конечных устройствах сети.

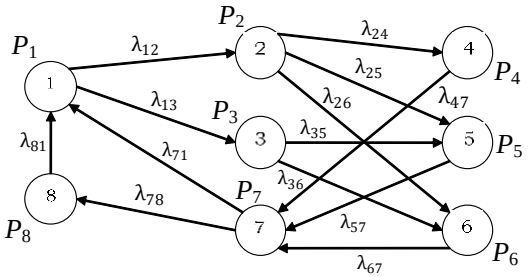

Рис. 1. Граф состояний процесса сетевой атаки, реализуемой деструктивными ботами

Fig. 1. The State Graph of a Network Attack Process Implemented by Destructive Bots

Представленная технология атаки позволяет осуществлять скрытый поиск подключенных в сеть хостов, с возможностью поиска открытых портов, что дает преимущества при обнаружении единичного агента, поскольку в целом распределенный атакующий комплекс продолжит достижение целевой функции. На граф-схеме обозначены следующие состояния: 1 – выбор объекта и портов для атаки; 2 – отправка корректных запросов; 3 – отправка некорректных запросов; 4 – принятие корректных данных; 5 – принятие отказа в данных; 6 – отсутствие ответа; 7 – анализ результатов; 8 – коррекция проведения атаки.

Эту граф-схему можно описать системой дифференциальных уравнений, на основании которых осуществить оценку вероятностей перехода из состояния в состояние:

$$\begin{cases} \frac{dP_1}{dt} = \lambda_{71}P_7(t) + \lambda_{81}P_8(t) - \lambda_{12}P_1(t) - \lambda_{13}P_1(t) \\ \frac{dP_2}{dt} = \lambda_{12}P_1(t) - \lambda_{24}P_2(t) - \lambda_{25}P_2(t) - \lambda_{26}P_2(t) \\ \frac{dP_3}{dt} = \lambda_{13}P_1(t) - \lambda_{35}P_3(t) - \lambda_{36}P_3(t) \\ \frac{dP_4}{dt} = \lambda_{24}P_2(t) - \lambda_{47}P_4(t) \\ \frac{dP_5}{dt} = \lambda_{25}P_2(t) + \lambda_{35}P_3(t) - \lambda_{57}P_5(t) \\ \frac{dP_6}{dt} = \lambda_{26}P_2(t) + \lambda_{56}P_3(t) - \lambda_{67}P_6(t) \\ \frac{dP_7}{dt} = \lambda_{47}P_4(t) + \lambda_{57}P_5(t) + \lambda_{67}P_6(t) - \lambda_{71}P_7(t) - \lambda_{78}P_7(t) \\ \frac{dP_8}{dt} = \lambda_{78}P_7(t) - \lambda_{81}P_5(t) \end{cases} . \quad (8)$$

Для нахождения оптимальной конфигурации многоагентной распределенной сети, позволяющей осуществить параллельность проведения атаки, было рассмотрено два варианта системы с различными начальными состояниями для распределенных агентов сети (рисунки 2, 3). В первом варианте распределенная атакующая система находится в частично спящем состоянии, когда всю работу выполняет лишь один агент. Второй вариант описывает поведение распределенной атакующей системы, находящейся в состоянии, когда функционирует множество агентов.

На рисунке 2 выбраны начальные состояния [1; 0; 0; 0; 0; 0; 0; 0] – начало атаки с первого состояния. Траектория развития атаки показала, что переходный процесс в целом завершен к 40-й секунде. На рисунке 3 выбраны начальные состояния [0,125; 0,125; 0,125; 0,125; 0,125; 0,125; 0,125; 0,125] – равномерное распределение начальных состояний. Траектория развития атаки показала, что переходный процесс в целом завершен к 40-й секунде. В обоих случаях наибольшую вероятность имеет 5-е состояние, наименьшую – 2-е и 4-е. Оценка переходного процесса, согласно графикам, позволяет предположить, что второй вариант более предпочтителен для реализации многоагентной распределенной сети, поскольку система приходит в устойчивое состояние раньше и соответственно вероятность обнаружения атаки ниже для второго случая. Оценка поведения кривых на рисунках 2, 3 показывает, что с момента завершения переходного процесса кривые имеют одинаковую динамику и вероятности практически сравниваются по значению.

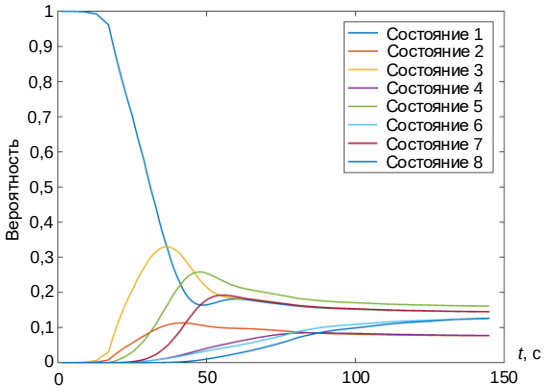

Рис. 2. Результат моделирования поведения системы с началом из первого состояния

Fig. 2. The Result of Modeling the Behavior of a System with a Start from the First State

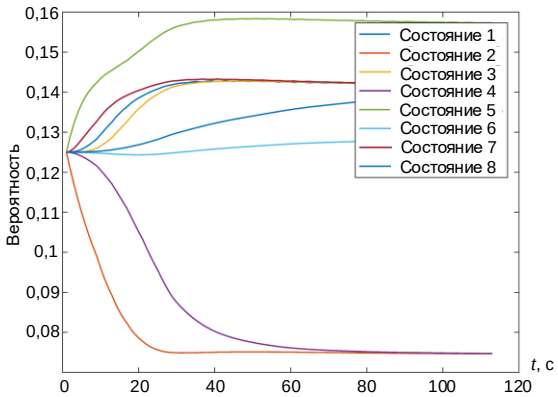

Рис. 3. Результат моделирования поведения системы с равномерным распределением начальных состояний

Fig. 3. The Result of Modeling the Behavior of the System with a Uniform Distribution of Initial States

Анализ вероятностей, полученных на разных временных промежутках показал, что в случае 1 имеются всплески вероятностей в состояниях 1, 2, 3, 5, 7. Для случая 2 глобальные всплески нехарактерны. Это позволяет оценить устойчивость процесса по изменению энтропии, вычисленной на основании полученных из (8) вероятностей по формуле $H = -\sum_{i=1}^{n} P_i \log_n P_i$. Анализ устойчивости, основанный на изменении энтропии, показал, что для случая 1 энтропия при переходном процессе нарастает, по окончании переходного процесса – слабо убывает. Для случая 2 – сразу слабо убывает.

Анализ вышеперечисленного позволяет сделать вывод, что случай 2 лучше подходит для формирования распределенных атакующих элементов на сети, и, вероятнее всего, будет использован злоумышленником. Рассмотрим поведение элементов при использовании средств защиты на атакуемой стороне. В 1-ом варианте – использование системы «антискан», блокирующей доступ к хосту при наличии попыток атакующей стороны сканировать порты и сервисы; во 2-ом варианте – системы молчаливого отказа, при котором некорректные запросы остаются без ответа. Смоделируем поведение системы с применением средств защиты, начальные состояния выберем с равномерным распределением (рисунки 4, 5).

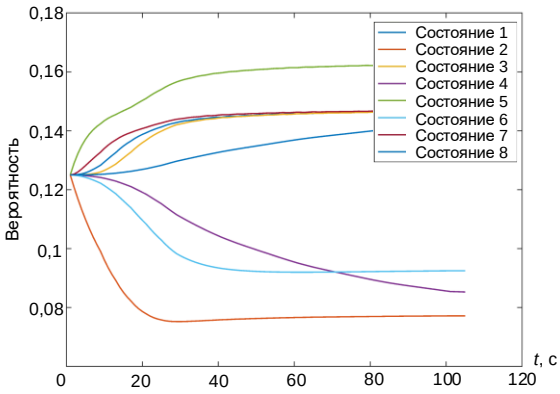

Рис. 4. Результат моделирования поведения системы с использованием системы блокирующей сканирование

Fig. 4. The Result of Modeling the Behavior of the System Using a System Blocking Scanning

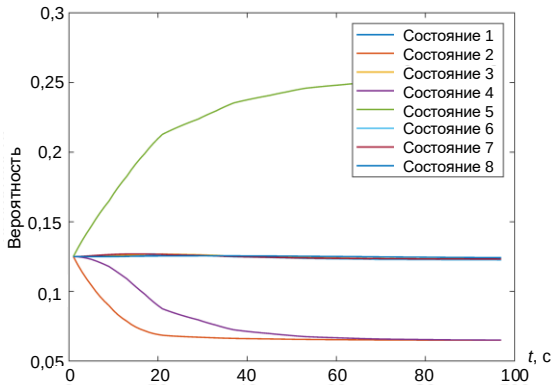

Рис. 5. Результат моделирования поведения системы с использованием «молчаливого отказа»

Fig. 5. The Result of Modeling the Behavior of the System Using "Silent Failure"

Поведение системы при применении средств блокирующей сканирование существенного влияния на динамику атаки не оказывает (рисунок 6). При использовании второго варианта защиты (рисунок 6) повышается вероятность нахождения процесса в состоянии 5 (принятие отказа в данных). В обоих случаях переходный процесс траектории развития атаки в целом завершается к 18-й секунде.

Моделирование динамики с применением энтропийного подхода к оценке устойчивости (см. рисунок 7) также не выявило показателей, по которым возможно было бы идентифицировать наличие атаки. Распределенные по сети агенты показывают достаточно устойчивое функционирование в период всей работы сети. При формировании атаки с первого состояния кривая поведения показывает динамику роста энтропии в самом начале атаки, однако затем процесс переходит в устойчивое состояние.

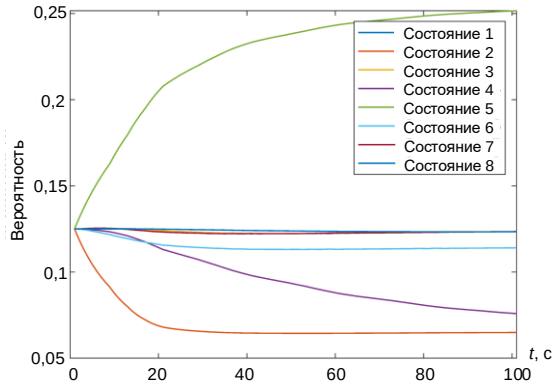

Рис. 6. Результат моделирования поведения системы при совместном применении средств защиты

Fig. 6. The Result of Modeling the Behavior of the System with the Combined Use of Protective Equipment

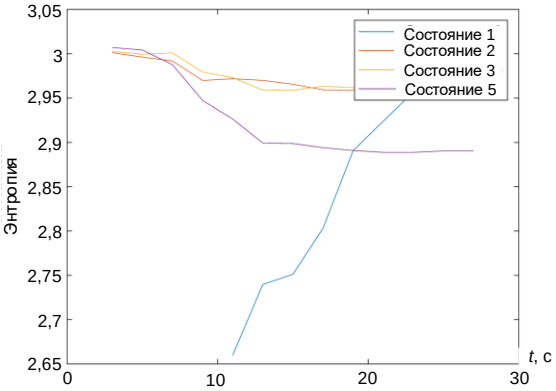

Рис. 7. Динамика изменения энтропии системы

Fig. 7. The Dynamics of Changes in the Entropy of the System

Анализ представленных результатов показал, что выявление распределенных атакующих элементов является достаточно сложной задачей. При этом в этих условиях первоочередной задачей является выявление координационного центра, осуществляющего атаку, поскольку его обнаружение позволит в значительной мере нейтрализовать деструктивные воздействия на сеть. Исходя из предположения,

что агент, проводящий координацию атаки, осуществляет прием и обработку информации о функционировании сети, рассмотрим его поведение в этих условиях. Работа элемента сети в штатном режиме функционирования «запрос-ответ» представлена на рисунке 8 верхней кривой (1), и позволяет сформировать пороговые показатели штатного режима.

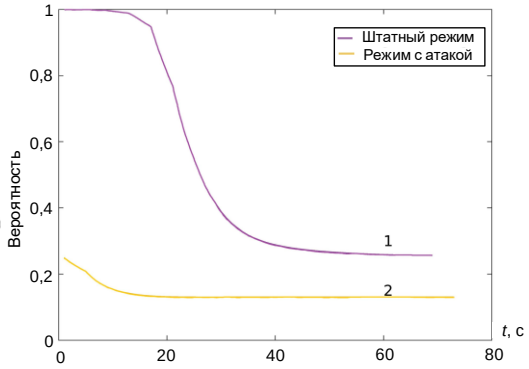

Рис. 8. Результат моделирования поведения агента

Fig. 8. The Result of Modeling Agent Behavior

Однако, как видно из поведения нижней кривой (2) в режиме атаки, кривая изменяет свое направление, и возникает разница отклонения от порогового значения, позволяющая сделать предположение о наличии атаки. Элемент, имеющий минимальное значение и будет являться координационным центром.

Дальнейший анализ функционирования сети целесообразно осуществлять в рамках поиска всего комплекса показателей, характеризующих ее работу [15, 16]. Это позволит не только осуществить поиск распределенных атакующих элементов сети, но сформировать комплекс мероприятий по защите как элементов, расположенных в сети, так и информации, циркулирующей в ней.

Заключение

Предлагаемая модель синтеза распределенных атакующих элементов, построенная с целью уменьшения объема вычислительных операций и увеличения времени реакции средств защиты, показала, что при правильной конфигурации системы управления атакой выявить их становится достаточно сложно. Выявление координационного центра возможно путем определения пороговых значений объема поступающей и отправляемой по сети информации. Дальнейшее направление работы целесообразно осуществлять в рамках развития динамических методов управления, позволяющих автоматизировать управление сетевой безопасностью [16, 17]. Это даст возможность не только оперативно учитывать изменения в законах функционирования сети, но и позволит обеспечить гибкость и снизить сложность решения задач прогнозирования сетевой безопасности и перейти к задачам построения моделей синтеза сетей как самовосстанавливающихся кибербезопасных объектов. Развитие этого направления в дальнейшей перспективе сформирует методы оперативного синтеза и реконфигурации сетей, адаптирующихся к текущим ситуациям. При данном подходе общая задача синтеза автоматически декомпозируется на ряд частных задач, каждая из которых имеет относительно низкий уровень сложности и свою область применения.

Список используемых источников

1. Мустафаев А.Г. Применение методов машинного обучения при анализе сетевого трафика // II Всероссийская научная конференция с международным участием (Тольятти, Россия, 22–24 апреля 2019). Информационные технологии в моделировании и управлении: подходы, методы, решения. Тольятти: Издатель Качалин Александр Васильевич, 2019. С. 198–205.

2. Минаев В.А., Королев И.Д., Петрова О.В., Овчаренко И.О. Моделирование системы защиты многоканальных автоматизированных комплексов от DDos-атак // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 1. С. 3–10. DOI:10.25586/RNU.V9187.19.01.P.003

3. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование: сборник научных трудов. Выпуск 16. Тюмень: Тюменский государственный университет, 2018. С. 347–356.

4. Яковлев Д.А., Синева И.С. Обнаружение сетевых аномалий на основе оценки интенсивности потоков в модели распада с целью защиты от распределенных атак // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 1. С. 41–44. DOI:10.24411/2072-8735-2018-10213

5. Ревняков Е.Н., Хмельникова О.А. Подбор приемлемого количества защищенных машин от DOS/DDOS атак при помощи теории игр // I Международная научно-практическая конференция. Наука XXI века: технологии, управление, безопасность (Курган, Россия, 26 сентября 2017). Курган: Курганский государственный университет, 2017 С. 373–379.

6. Косенко М.Ю. Интеллектуальный анализ данных в задаче обнаружения ботнетов // Вестник УрФО. Безопасность в информационной сфере. 2016. № 1(19). С. 22–29.

7. Тарасов Я.В. Методический подход к обнаружению DDos-атак малой мощности // Восьмая всероссийская научно-техническая конференция НУК «Информатика и системы управления» (Москва, Россия, 6–7 декабря 2017). Безопасные информационные технологии. М.: МГТУ им. Н.Э. Баумана, 2017. С. 479–482.

8. Sun F., Pi J., Lv J., Cao T. Network Security Risk Assessment System Based on Attack Graph and Markov Chain // Journal of Physics: Conference Series. 2017. Vol. 910(1). DOI:10.1088/1742-6596/910/1/012005

9. Корниенко А.А., Никитин А.Б., Диасамидзе С.В., Кузьменкова Е.Ю. Моделирование компьютерных атак на

распределенную информационную систему // Известия Петербургского университета путей сообщения. 2018. Т. 15. № 4. С. 613–628.

10. Vorobiev V., Fatkieva R., Evnevich E. Security Assessment of Robotic System with Inter-Machine Interaction // Proceedings of the International Russian Automation Conference (RusAutoCon, Sochi, Russia, 9–16 September 2018). IEEE, 2018. DOI:10.1109/RUSAUTOCON.2018.8501753

11. Потапов В.И. Противоборство технических систем в конфликтных ситуациях: модели и алгоритмы. Омск: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Омский государственный технический университет", 2015. 168 с.

12. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50–99. DOI:10.24411/2410-9916-2019-10403

13. Govindasamy J., Punniakodi S. Optimised watchdog system for detection of DDOS and wormhole attacks in IEEE802.15.4-based wireless sensor networks // International Journal of Mobile Network Design and Innovation. 2018. Vol. 8. Iss. 1. PP. 36–44.

14. Фаткиева Р.Р., Рыжков С.Р. Оценка нарушения периметра информационной безопасности в облачной среде // Информационные технологии. 2018. Т. 24. № 12. С. 791–798. DOI:10.17587/it.24.791-798

15. Marnerides A.K., Pezaros D.P., Hutchison D. Internet traffic characterisation: Third-order statistics & higher-order spectra for precise traffic modeling // Computer Networks. 2018. Vol. 134. PP. 183–201. DOI:10.1016/j.comnet.2018.01.0500

16. Queiroz W., Capretz M.A.M., Dantas M. An approach for SDN traffic monitoring based on big data techniques // Journal of Network and Computer Applications. 2019. Vol. 131. PP. 28–39. DOI:10.1016/j.jnca.2019.01.016

17. Liu Y., Lu Y., Qiao W., Chen X. A Dynamic Composition Mechanism of Security Service Chaining Oriented to SDN/NFV-Enabled Networks // IEEE Access. 2018. Vol. 6. PP. 53918–53929. DOI:10.1109/ACCESS.2018.2870601

* * *

A Model of Synthesis of Distributed Attacking Elements in a Computer Network

M. Petrov[1], **R. Fatkieva**[1]

[1]St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
St. Petersburg, 199198, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-2-113-120
Received 28th April 2020
Accepted 25th June 2020

For citation: Petrov M., Fatkieva R. A Model of Synthesis of Distributed Attacking Elements in a Computer Network. *Proc. of Telecom. Universities.* 2020;6(2):113–120. (in Russ.) DOI:10.31854/1813-324X-2020-6-2-113-120

Abstract: *An approach to predicting the development of attacks on network resources using distributed attacking tools is presented. Distinctive features of attack scenarios are shown. A model of the functioning of a network with distributed attacking elements is described. It is shown that dynamics modeling using the entropy approach to stability assessment does not make it possible to identify the presence of an attack. A method for detecting a focal point carrying out an attack is proposed.*

Keywords: *recognition, space object, modeling, radar image, correlation function.*

References

1. Mustafaev A.G. The Application of Machine Learning Methods in the Analysis of Network Traffic. *Proceedings of the IId Information Technologies in Modeling and Management: Approaches, Methods, Solutions, 22–24 April 2019, Tolyatti, Russia*. Tolyatti: Izdatel Kachalin Aleksandr Vasilyevich Publ.; 2019. p.198–205. (in Russ.)

2. Minaev V.A., Korolev I.D., Petrova O.V., Ovcharenko I.O. Protection System Modelling of Multi-Channel Automated Complexes from DDos Attacks. *Vestnik RosNOU, Complex systems: models, analysis, management series.* 2019;1:3–10. (in Russ.) DOI:10.25586/RNU.V9187.19.01.P.003

3. Savchenko E.V., Nissenbaum O.V. Botnet Attacks on IOT Devices. *Proceedings of the Mathematical and Information Modeling*. Tyumen, Russia. Tyumen: University of Tyumen Publ.; 2018. vol.16. p.347–356. (in Russ.)
4. Yakovlev D.A., Sineva I.S. Network anomaly detection based on flow intensity measuring in the decay model for DDoS protection. *T-Comm*. 2019;13(1):41–44. (in Russ.) DOI:10.24411/2072-8735-2018-10213
5. Revnacov E.N., Hmelnikova O.A. Selection of an Acceptable Number of Machines Protected from DOS/DDOS Attacks Using Game Theory. *Proceedings of the I international scientific and practical conference, 26 September 2017, Kurgan, Russia. Science of the XXI century: Technologies, Management, Security*. Kurgan: Kurgan State University Publ.;2017. p.373–379. (in Russ.)
6. Kosenko M.Yu. Data mining in the problem of detecting botnets. *UrFR Newsletter. Information Security*. 2016;1(19):22–29. (in Russ.)
7. Tarasov Ya.V. Methodological approach to detecting low-power DDos. *Proceedings of the 8th All-Russian Scientific and Technical Conference: NUK "Informatics and Control Systems", 6–7 December 2017, Moscow, Russia. Secure Information Technologies*. Moscow: Bauman Moscow State Technical University Publ.; 2017. p.479–482. (in Russ.)
8. Sun F., Pi J., Lv J., Cao T. Network Security Risk Assessment System Based on Attack Graph and Markov Chain. *Journal of Physics: Conference Series*. 2017;910(1). DOI:10.1088/1742-6596/910/1/012005
9. Kornienko A.A., Nikitin A.B., Diasamidze S.V., Kuz'menkova E.Yu. Simulation of Computer Attacks on Distributed Software. *Proceedings of Petersburg Transport University*. 2018;15(4):613–628. (in Russ.)
10. Vorobiev V., Fatkieva R., Evnevich E. Security Assessment of Robotic System with Inter-Machine Interaction. *Proceedings of the International Russian Automation Conference, RusAutoCon, 9–16 September 2018, Sochi, Russia*. IEEE; 2018. DOI:10.1109/RUSAUTOCON.2018.8501753
11. Potapov V.I. *Confrontation of Technical Systems in Conflict Situations: Models and Algorithms*. Omsk: Omsk State Technical University Publ.; 2015. 168 p. (in Russ.)
12. Maximov R.V., Orekhov D.N., Sokolovsky S.P. Model and Algorithm of Client-Server Information System Functioning in Network Intelligence Conditions. *Systems of Control, Communication and Security*. 2019;4:50–99. (in Russ.) DOI:10.24411/2410-9916-2019-10403
13. Govindasamy J., Punniakodi S. Optimised watchdog system for detection of DDOS and wormhole attacks in IEEE802.15.4-based wireless sensor networks. *International Journal of Mobile Network Design and Innovation*. 2018;8(1):36–44.
14. Fatkieva R.R., Ryzhkov S.R. Assessment of Violations of Information Security Perimeter in the Cloud. *Information Technologies*. 2018;24(12):791–798. (in Russ.) DOI:10.17587/it.24.791-798
15. Marnerides A.K., Pezaros D.P., Hutchison D. Internet traffic characterisation: Third-order statistics & higher-order spectra for precise traffic modeling. *Computer Networks*. 2018;134:183–201. DOI:10.1016/j.comnet.2018.01.0500
16. Queiroz W., Capretz M.A.M., Dantas M. An approach for SDN traffic monitoring based on big data techniques. *Journal of Network and Computer Applications*. 2019;131:28–39. DOI:10.1016/j.jnca.2019.01.016
17. Liu Y., Lu Y., Qiao W., Chen X. A Dynamic Composition Mechanism of Security Service Chaining Oriented to SDN/NFV-Enabled Networks. *IEEE Access*. 2018;6:53918–53929. DOI:10.1109/ACCESS.2018.2870601

Сведения об авторах:

ПЕТРОВ Михаил Юрьевич — ведущий программист лаборатории Информационно-вычислительных систем и технологии программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, miha@iias.spb.su
https://orcid.org/0000-0002-2711-8469

ФАТКИЕВА Роза Равильевна — кандидат технических наук, доцент, старший научный сотрудник лаборатории Информационно-вычислительных систем и технологии программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, rikki2@yandex.ru
https://orcid.org/0000-0003-4065-9611