УДК 004.8+519.7 DOI: 10.18698/0236-3933-2022-3-61-77

СОВРЕМЕННЫЕ ИММУНОЛОГИЧЕСКИЕ МОДЕЛИ И ИХ ПРИЛОЖЕНИЯ

Ю.А. Скобцов ya_skobtsov@list.ru

ГУАП, Санкт-Петербург, Российская Федерация

Аннотация

Рассмотрены основные модели и алгоритмы искусственных иммунных систем, которые по своей парадигме близки к эволюционным вычислениям и используются при поиске потенциальных решений, каждое из которых представлено искусственным лимфоцитом. При этом также, как особь в эволюционных вычислениях, искусственный лимфоцит кодируется чаще всего двоичной строкой или вектором вещественных чисел. Среди основных моделей искусственных иммунных систем алгоритм клонального отбора близок к эволюционной стратегии эволюционных вычислений, но использует более мощные операторы мутации и применяется в основном для решения задач численной и комбинаторной оптимизации. Алгоритм отрицательного отбора, основанный на принципе распознавания «свой»-«чужой» в иммунной системе, наиболее популярен в приложениях. Приведены два аспекта алгоритма: 1) базовая концепция — использование дополнения множества «своих» клеток; 2) цель — научиться различать клетки «свой»-«чужой», в то время как доступны только образцы «своих» клеток. Рассмотрены непрерывные и дискретные сетевые модели, представляющие собой регулируемые сети молекул и клеток. Отмечены преимущества и недостатки приведенных моделей и их применение в области компьютерной безопасности, робототехники, обнаружения мошенничества и неисправностей, интеллектуального анализа данных, анализа текста, распознавания образов и изображений, биоинформатики, игр, планирования и т. д.

Ключевые слова

Искусственные иммунные системы, клональный отбор, отрицательный отбор, идиопатическая сеть, компьютерная безопасность

Поступила 27.05.2022
Принята 14.06.2022

Введение. В последние десятилетия быстро развивается новое направление в теории и практике искусственного интеллекта — биоинспирированные (вдохновленные природой) методы и алгоритмы, которые при поиске ре-

шений поставленной задачи используют модели некоторых биологических систем. Самыми известными, популярными и старыми из них являются искусственные нейронные сети, которые зародились в сороковых годах прошлого века на основе простейших моделей нейронов и нервной системы. Это направление прошло сложный путь развития и сейчас широко применяется на практике. Достаточно популярными также являются эволюционные вычисления (ЭВ) (генетические алгоритмы, генетическое программирование, эволюционное программирование, эволюционные стратегии). Этот термин обычно используется для общего описания алгоритмов поиска, оптимизации или обучения, основанных на некоторых формализованных принципах естественного эволюционного отбора. На сегодняшний день разработано более 100 различных алгоритмов (метаэвристик) на основе биологических (и не только) систем и число их продолжает расти. В настоящей работе рассмотрено одно из самых интересных и перспективных направлений — искусственные иммунные системы (ИИС), которые разрабатываются на основе моделей «своего» биологического прототипа — естественной иммунной системы [1, 2].

Искусственные иммунные системы или иммунологические вычисления быстро развиваются. Растет интерес к разработке вычислительных моделей, основанных на иммунологических принципах. Некоторые модели имитируют абстрактные механизмы в биологической иммунной системе, чтобы лучше понять ее естественные процессы, и моделируют ее динамическое поведение в присутствии антигенов или патогенов. Другие делают упор на проектирование вычислительных алгоритмов, методов, использующих упрощенные концепции различных иммунологических процессов и функций. Отметим, что ИИС (по крайней мере, некоторые модели, например алгоритм клонального отбора) по своей идеологии достаточно близки к ЭВ [3]. При поиске решения ИИС используют популяцию потенциальных решений, каждое из которых представляется искусственным лимфоцитом (ИЛ) — аналогом особи в ЭВ. Как и особь в ЭВ, ИЛ представляется (кодируется) чаще всего двоичной строкой или вектором вещественных чисел. В ИИС при формировании следующей популяции применяются более продвинутые операторы мутации. Качество ИЛ оценивается с помощью функции аффинности (аналог фитнесс-функции в ЭВ) [2].

Для построения модели ИИС есть несколько основных аспектов, которые необходимо учитывать [2]:

– должны быть обученные детекторы (ИЛ), которые обнаруживают «чужие» образы (паттерны) с определенной аффинностью (подобием);

– ИИС может потребоваться хорошее хранилище для «своих» или «чужих» образов для обучения ИЛ;

– необходим инструмент (средство) измерения подобия (аффинности) между ИЛ и шаблоном; измеренная аффинность должна показывать степень обнаружения образа;

– чтобы измерить подобие (аффинность), представление (кодирование) образов и ИЛ должны иметь одинаковую структуру;

– необходимо измерять близость (аффинность) между двумя ИЛ; измеренная близость указывает, в какой степени ИЛ могут связываться друг с другом для формирования сети;

– ИИС должна иметь память, создаваемую ИЛ, которые часто обнаруживают паттерны, не связанные с собой;

– когда ИЛ обнаруживает «чужие» образы, их можно клонировать, а клоны — мутировать, чтобы иметь больше разнообразия в пространстве поиска.

Алгоритм клонального отбора. Алгоритм основан на теории клонального отбора [4], которая предполагает, что для разрушения или нейтрализации антигена (болезнетворного микроорганизма) используются лимфоциты (*B*- и *T*-клетки). Когда лимфоцит выбран и связан с антигеном, он размножается и дифференцируется в плазматические клетки и клетки памяти. Плазматические клетки имеют короткую продолжительность жизни и производят большое число молекул антител, тогда как клетки памяти живут в течение длительного периода времени, ожидая в будущем тот же самый антиген. Основанная на принципах эволюционной теории естественного отбора Дарвина эта теория использует клонирование отобранных лимфоцитов. Далее клоны подвергаются мутации, что повышает эффективность борьбы с антигеном. Псевдокод алгоритма клонального отбора приведен далее.

Begin

Инициализация: определение параметров таких, как размер репертуара M, критерий останова (например, максимальное число поколений maxgen), фактор клонирования β и т. д.

Генерация случайного начального репертуара антител, оценка аффинности антител, gen = 0

While *(не выполнен критерий останова — например, gen > maxgen)*

Генерация каждым антителом round (βM) идентичных клонов.

Таким образом, увеличивается размер репертуара после клонирования aN_c следующим образом:

$$N_c = \sum_{i=1}^{M} round(\beta M) + M$$

Выполнение для клонов соматической гипермутации (т. е. степень мутации похожего клона (имеющего большую аффинность) меньше, в то время как число исходных антител сохраняется без изменений; этот этап также называется процессом созревания аффинности).

Определение меры аффинности мутантов.

Выбор антител с самыми высокими показателями аффинности среди N_c-антител и отбрасывание остальных

$$gen = gen + 1$$

End

Output: *сгенерированный репертуар антител*

Алгоритм клонального отбора похож на метод эволюционных стратегий ЭВ с более развитым оператором мутации. Его можно грубо рассматривать как параллельную версию $1 + round\ (\beta M)$ — эволюционную стратегию [3] с адаптивным контролем мутаций. Разработаны версии клонального отбора как с дискретным, так и с вещественным кодированием [4, 5]. Этот алгоритм чаще всего применяется для решения задач оптимизации.

Алгоритм отрицательного отбора (АОО). Алгоритм [6, 7] основан на принципе распознавания «свой»-«чужой» в иммунной системе и наиболее популярен в приложениях ИИС. В естественной иммунной системе такое распознавание обеспечивается *Т*-лимфоцитами и другими клетками, имеющими на своей поверхности рецепторы, способные обнаруживать чужеродные белки (антигены). Как отличить «свои» белки от патогенных «чужих» белков с помощью *Т*-клеток? Попадая в тимус (вилочковую железу — центральный орган иммунной системы), *Т*-клетки подвергаются отрицательному отбору, который заключается в том, что клетки, вступившие в реакцию с собственными белками, уничтожаются, а остальные (не образующие с ними связей) получают возможность покинуть тимус. Затем эти *Т*-клетки циркулируют по всему организму и выполняют функцию защиты от антигенов.

Аналогично действует АОО, случайным образом создавая детекторы и удаляя те из них, которые распознают «свои» клетки, так что остающиеся детекторы могут обнаруживать любые «чужие» клетки. Основная

цель АОО — покрытие пространства «чужих» (антигенов) набором детекторов.

Два важнейших аспекта АОО заключаются в следующем:

1) базовая концепция алгоритма — использование дополнения к множеству «своих» (клеток);

2) цель состоит в том, чтобы научиться различать клетки «свой»–«чужой», в то время как доступны только образцы «своих» клеток.

Алгоритм отрицательного отбора состоит из двух этапов [1, 2]: 1) генерация детекторов; 2) обнаружение «чужих». На первом этапе генерируется набор детекторов некоторым рандомизированным процессом, который использует в качестве входных данных множество «своих» — Sself. Кандидаты в детекторы, которые обнаруживают любые «свои» элементы, удаляются, а которые не распознают «своих» сохраняются. Псевдокод простейшего алгоритма отбора детекторов приведен далее.

```
input: Sself — множество «своих» элементов
Begin
    популяция = {}
    While (не выполнен критерий останова)
        Новое_антитело=случайная_генерация_антитела
        соответствие = False
        For каждого { s | s ∈ Sself }
            If есть соответствие (s, новое_антитело)
                соответствие = True
            End
If нет соответствия
популяция = популяция ∪ новое_антитело
    End
  End
End
Output: множество детекторов
```

Для генерации детекторов при решении реальных задач используются различные алгоритмы: случайные, жадные, эволюционные, динамического программирования и другие, имеющие различную сложность и адекватность [2, 8]. Временная и пространственная сложности основных алгоритмов генерации детекторов показаны в табл. 1, где m — мощность алфавита; N_S — число элементов в множестве «свои»; l — длина строки; r — порог соответствия; N_R — число детекторов.

Таблица 1

Сложность генерации детекторов

Алгоритм	Время	Пространство
Исчерпывающий поиск	$\mathrm{O}\left(m^1 N_S\right)$	$\mathrm{O}\left(l N_S\right)$
Линейный	$\mathrm{O}\left(\left(l-r+1\right)N_S m^r\right)+$ $+\,\mathrm{O}\left(l-r+1\right)m^r + \mathrm{O}\left(l N_R\right)$	$\mathrm{O}\left(\left(l-r+1\right)^2 m^r\right)$
Жадный	$\mathrm{O}\left(\left(l-r+1\right)N_S m^r\right)+$ $+\,\mathrm{O}\left(\left(l-r+1\right)m^r\ \right)\left(N_R\right)$	$\mathrm{O}\left(\left(l-r+1\right)^2 m^r\right)$
N_S-мутация	$\mathrm{O}\left(m^1 N_S\right) + \mathrm{O}\left(N_R m^r\right) + \left(N_R\right)$	$\mathrm{O}\left(l\left(N_S + N_R\right)\right)$

На этапе обнаружения множество детекторов (сгенерированное на первом этапе и сохраненное для дальнейшего применения) используется для проверки соответствия новых входящих образцов «своим» или «чужим» экземплярам. Если входной образец соответствует детектору, он идентифицируется как часть «чужих», что в большинстве приложений означает, что имеет место аномалия/изменение. Конкретный АОО характеризуется тем, как представлены детекторы, какие правила используются для определения соответствия между образцом и детекторами, и механизмы для создания и удаления детекторов «свой»-«чужой». В большинстве работ по АОО потенциальные решения кодируются либо двоичными строками, либо вещественными векторами, хотя применяются и более сложные конструкции.

Положительный отбор. В естественной иммунной системе также используется положительный отбор, хотя и не так широко, как отрицательный. Положительный отбор выполняется на основе рецепторов фильтра, обнаруженных на поверхности незрелых *T*-клеток. Рецептор — это молекула MHC (Major Histocompatibility Complex), которая позволяет организму отфильтровывать еще не созревшие *T*-клетки. Положительный отбор работает аналогично АОО, но вместо удаления антител из популяции, если они совпадают, антитела добавляются в репертуар. В отличие от отрицательного отбора методы положительного отбора широко используются в распознавании образов, кластеризации и других областях, где они генерируют набор детекторов, которые отображают (распознают) «свои» образы (вместо «чужих»). В этом случае модель множества «своих» (обучающие данные) используется для классификации выборки как части «своих» или «чужих». Простая модель положительного отбора может быть построена с использованием подхода ближайшего соседа. Если образ находится в окрестности эталона, то он отмечается как принадлежащий этому мно-

жеству. Как правило, положительный детектор определяет окрестности, предполагая гиперсферу с определенным радиусом с центром в каждом «своем» образе. Детекторы можно определить и более сложным способом, используя некоторый алгоритм кластеризации на элементах множества «своих». Таким образом, распознаваемая точка может быть классифицирована как принадлежащая к кластеру путем измерения расстояния до него, например в метрике Минковского. Сравнение методов отрицательного и положительного отборов выполнено в [2, 9]. Хотя метод положительного отбора дал более точные результаты, он более затратный по времени и памяти по сравнению с методом отрицательного отбора. Оба подхода используются в разных условиях. Многочисленные приложения с большим числом данных «своих» кажутся более подходящими для метода отрицательного отбора.

Сетевые модели. Такие модели предполагают гипотезу, согласно которой иммунная система представляет собой регулируемую сеть молекул и клеток, распознающих друг друга даже при отсутствии антигена [10], их часто называют идиотипическими сетями, которые служат основой для изучения поведения иммунной системы. Сетевые модели иммунной системы можно разделить на две категории: непрерывные и дискретные модели [1, 2]. В непрерывных моделях предполагается, что иммунный ответ является непрерывным, в отличие от дискретных моделей, где это происходит в дискретных временных шагах. Непрерывные модели на основе дифференциальных уравнений не фокусируются на структуре иммунной системы, а рассматривают концентрации антител и чужеродных антигенов, хотя они предполагают, что все антитела взаимодействуют друг с другом, и антигены также взаимодействуют со всеми антителами. Изменение концентрации конкретного антитела x_i представляется как сумма dx_i / dt = внутренняя сетевая динамика + динамика, управляемая антигеном. Первое слагаемое моделирует взаимодействие между антителами, а второе слагаемое — стимуляцию антитела антигенами.

В модели Ерне [11] для описания изменения концентрации лимфоцитов определенного типа используется следующее уравнение:

$$\frac{dx_i}{dt} = x_i \sum_{i=1}^{N} f\left(E_j, K_j, t\right) - x_i \sum_{i=1}^{N} g\left(I_j, K_j, t\right) + k_1 - k_2 x_i,$$

где первое слагаемое представляет собой общую стимуляцию лимфоцитов типа i посредством возбуждения сигналов в виде суммы возбуждающих сигналов, полученных от стимулирующих лимфоцитов. Соответственно $f\left(E_j, K_j, t\right)$ является мерой возбуждения сигналов от идиотипов в E_j

на лимфоците типа i в момент времени t; здесь K_j — константа, связанная с силой аффинности между лимфоцитами типа i и идиотипами в E_j. Аналогичным образом второе слагаемое выражает общий эффект ингибирующих сигналов от других лимфоцитов на лимфоцит типа I. Таким образом, I_j выражает лимфоцит, который (путем объединения сайтов) распознает идиотипы на клетках типа I. Кроме того, k_1 — это скорость, с которой лимфоциты типа i попадают в сеть, а k_2 — отношение, определяющее естественную смертность лимфоцитов типа I при отсутствии антигена.

В этой модели дифференциальное уравнение описывает изменение концентрации лимфоцитов каждого типа. Таким образом, сеть демонстрирует динамическое поведение даже при отсутствии стимулирующих антигенов. Чтобы описать динамическое поведение чужеродного антигена, необходимо включить дополнительный термин, представляющий взаимодействие соответствующего лимфоцита типа *I* с внешними антигенами.

Однако дискретные модели обычно представляют собой абстрактные функциональные модели, которые используются ИИС, их целью является решение реальных вычислительных проблем. Дискретные модели рассматривают ИИС как множество *B*-клеток, которые взаимодействуют друг с другом в соответствии со своей аффинностью. Первая дискретная модель ИИС [12] также рассматривает ИИС как множество *B*-клеток, которые взаимодействуют друг с другом в соответствии со своей аффинностью; *B*-клетки представляются в виде двоичных строк, следуя некоторым более ранним работам [10]. Поэтому аффинность между *B*-клетками определяется на основе расстояния Хэмминга. Если стимуляция *B*-клеток чужеродными антигенами выше определенного порога, то они клонируются и мутируют. Клонирование производит определенное число точных копий *B*-клетки. Однако число копий зависит от уровня стимуляции *B*-клетки. Кроме того, в операторе простой подстановки небольшая (менее половины) часть подстроки, представляющая *B*-клетку, заменяется соответствующими элементами другой случайным образом выбранной *B*-клетки. Введены также три типа операторов мутации: многоточечная мутация, регенерация подстроки и простая замена. Однако каждый раз только один оператор применяется к клону случайным образом. При многоточечной мутации каждый элемент антитела мутирует с определенной вероятностью. При этом в подстроке регенерации случайным образом выбирается подстрока паратопа антитела и заменяется случайно сгенерированной строкой. Кроме приведенных основных моделей, используются и многие другие, с которыми можно ознакомиться, например, в [2, 13, 14].

Сравнение основных моделей. Наиболее распространенные вычислительные модели ИИС приведены в табл. 2, где показано использование конкретных иммунологических концепций в различных моделях и их основные приложения.

Приложения. В качестве инструмента ИИС применяются в реальных приложениях в следующих областях: компьютерной безопасности, обнаружении мошенничества, робототехнике, обнаружении неисправностей, интеллектуальном анализе данных, анализе текста, распознавании образов и изображений, биоинформатике, играх, планировании, оптимизации, классификации, кластеризации, обнаружении аномалий, машинном обучении, адаптивном управлении и ассоциативной памяти и других областях, которые приведены в табл. 2. Искусственные иммунные системы также применяются в сочетании с другими методами, такими как генетические алгоритмы, нейронные сети, нечеткая логика и роевой интеллект.

Общее описание процесса решения с использованием моделей иммунной системы представлено некоторыми приложениями общего назначения, например *ARTIS* [15] и *LISYS* [16]. Кроме того, далее кратко описаны некоторые применения ИИС, чтобы продемонстрировать, как эти методы могут использоваться для решения реальных проблем.

Искусственная иммунная система *ARTIS* разработана в 2000 г. [15] и является ИИС, которая моделирует многие процессы и свойства системы позвоночных, включая некоторые концепции и алгоритмы, приведенные ранее. Цель *ARTIS* — указать элементы общей адаптивной распределенной системы без ссылки на какие-либо конкретные приложения. Затем эти общие элементы должны быть конкретизированы в соответствии с характеристиками приложения. В качестве примера этой конкретизации рассматривается *LISYS* [16] (легкая система обнаружения вторжений) — система обнаружения вторжений в сеть, основанная на *ARTIS*. Каждый узел в защищаемой системе представляет собой сетевой компьютер, который имеет локальную коллекцию рецепторов и локальный уровень чувствительности. Антигены, которые должны контролироваться детекторами, — это строки, содержащие информацию о сетевом трафике, влияющем на защищаемые узлы. Обнаружение аномальных строк приводит к генерации тревоги для человека оператора.

Версия *LISYS* для мониторинга сетевого трафика использована в [17]. Система использовала АОО для создания зрелых 49-разрядных двоичных детекторов, т. е. триплетов, представляющих собой соединения протокола управления передачей TCP (Transmission Control Protocol), который был проверен на наличие соединений, собранных в течение периода обучения.

Таблица 2

Иммунологические вычислительные модели и концепции

Критерий	Клональный отбор	Отрицательный отбор	Сетевые модели
Иммунологические концепции и сущности	Клональное расширение, созревание аффинности, *B*-клетка	Распознавание «свой»-«чужой» на основе *T*-клеток	Идиотипическая сеть, иммунная память, *B*-клетка
Типы данных	Двоичные строки, вещественные векторы		
Элементы	Эпитопы, клетки плазмы, клетки памяти	Детекторы, антиген, рецепторы	*B*-лимфоциты, *Y*-антитела
Операции	Клональный отбор, соматическая мутация, вычисление аффинности, пролиферация, дифференциация	Отрицательный отбор, соответствие, связывание, генерация детекторов, вычисление аффинности	Клонирование, мутация, отсечение и выращивание дуг на основе аффинности, стимуляция и супрессия для стабилизации сети
Преимущества	Повышение разнообразия репертуара защищает от ранее невстречавшихся антигенов и формирует более эффективный вторичный ответ. Хорошее распараллеливание. Мало параметров пользователя, невысокая сложность	Способность различать «своих» и «чужих». Не нужны предварительные знания о множестве «чужих» элементов. Наличие алгоритмов генерации детекторов различной сложности. Способность к обнаружению аномалий. Хорошее распараллеливание	Постоянная адаптация сети для поддержания устойчивого состояния. Гибкий механизм выбора, автономный и полностью децентрализованный. Стимуляция и подавление формируют сеть с параллельной распределенной обработкой и стабилизируют сеть

Недостатки	Встречается преждевременная сходимость к локальным экстремумам. Желательна точная оценка мощности репертуара. Слабая обратная связь	Неуместен, если множество «своих» мало или пространство поиска бесконечно. Стандартный алгоритм генерации детекторов имеет экспоненциальную сложность. Требуется обычное программное обеспечение для итеративного увеличения образцов «своих»	Ограниченная применимость — большие накладные расходы, вычислительная сложность и непонимание их динамики. Применение свойств возбуждения и подавления сетевой модели поддерживается обычным программным обеспечением
Приложения	Численная и комбинаторная оптимизация, распознавание образов, классификация, машинное обучение, классификация числовых данных. Гибкая альтернатива генетическому алгоритму	Обнаружение аномалий, неисправностей, изменений, компьютерная безопасность, защита от вирусов и сетевых мошенничества и вторжений, двоичная классификация	Обучение (с учителем и без), управление, кластеризация, извлечение данных, классификация текстов, распознавание образов

Созревшие детекторы затем были распределены на каждом хосте в действующий. При этом разнообразие создается через каждый хост, независимо реагирующий на «свой» и «чужой» (нормальный и ненормальный).

Компьютерная безопасность во многих отношениях аналогична биологической защите [6, 18, 19]. Таким образом, можно извлечь уроки и полезные знания из естественной иммунной системы, чтобы повысить цифровой иммунитет. Большинство первых работ ИИС посвящено использованию некоторых иммунологических моделей для разработки защиты цифровых систем [6, 7, 19]. В ИИС использовались различные аспекты защиты данных и поиска аномалий для обеспечения универсальной системы защиты и улучшения существующих систем компьютерной безопасности. Безопасность компьютерных систем зависит от таких действий, как обнаружение несанкционированного использования вычислительной техники, поддержание целостности данных, файлов и предотвращение распространения компьютерных вирусов. Впервые в [6] предложено использовать отрицательный отбор в компьютерной безопасности. Здесь рассматривалась задача защиты компьютерных систем от вредных вирусов как частный случай общей проблемы распознавания «свой» (законные пользователи, целостные данные и т. д.) и «чужой» (опасный, несанкционированные пользователи, вирусы и другие вредоносные агенты). Этот метод должен был стать дополнением к более традиционным методам криптографической и детерминированной аутентификации файлов для проблемы обнаружения компьютерных вирусов.

Еще один иммунологически вдохновленный подход (основанный на гипотезе вторжения) для обнаружения вирусов предложен в [20]. При таком подходе известные вирусы обнаруживаются по их последовательностям компьютерных кодов (сигнатурам), а неизвестные вирусы по их необычному поведению в компьютерной системе. Эта система обнаружения вирусов постоянно сканирует программное обеспечение компьютера на наличие типичных признаков вирусной инфекции. Эти сигнатуры вызывают запуск «программ-приманок», единственной целью которых является заражение вирусом.

Автоматическая система обнаружения и реагирования для выявления вредоносного самораспространяющегося кода и предотвращения его распространения CARDINAL (Cooperative automated worm, алгоритм ответа и обнаружения) предложена в [21]. Этот метод основан на понятиях дифференциации состояний *T*-клеток. В частности, определены три ключевых свойства *T*-клеток: 1) пролиферация *T*-клеток для оптимизации числа опрошенных хостов; 2) дифференциация *T*-клеток для оценки серьезности

и достоверности атаки; 3) модуляция и взаимодействие *T*-клеток, чтобы сбалансировать локальную и одноранговую информации. Цель работы — использование разнообразных типов *T*-клеток для работы в качестве совместной автоматизированной системы обнаружения и реагирования на вирусы типа «черви».

Применение концепции ИИС к решению проблемы обнаружения и устранения неисправностей в цифровых электронных системах рассмотрено в [22]. Классическими подходами к обнаружению и устранению неисправностей в ИИС являются резервирование и добавление систем защиты, которые проверяют и, возможно, исправляют техническое состояние системы. Подход на основе иммунотроники определяет систему такого же типа, но использует концепцию ИИС для распознавания «свой»-«чужой» и автоматизации генерации критериев проверки, используемых для защиты системы. Этот подход применим к моделям конечного автомата — класса систем, в которых работа моделируется в терминах состояний и переходов между ними, охватывающих большинство существующих электронных систем.

В этом случае множество «своих» может быть определено как набор строк, которые представляют собой законные переходы между состояниями автомата. Например, строки могут быть сформированы путем конкатенации строки, содержащей значения текущих входных данных, текущее состояние, и строки, которая содержит следующее состояние, сгенерированное автоматом .

Заключение. Модели ИИС активно развиваются и применяются в реальных приложениях во многих областях. Прежде всего это компьютерная безопасность, обнаружение мошенничества, робототехника, обнаружение неисправностей, интеллектуальный анализ данных и т. п. Они также применяются в сочетании с другими методами вычислительного интеллекта, такими как эволюционные алгоритмы, нейронные сети, нечеткая логика и роевой интеллект. Гибридные системы способны получить преимущества благодаря индивидуальным сильным сторонам и устранить недостатки различных парадигм, таким образом предлагая мощные алгоритмы для решения сложных проблем.

ЛИТЕРАТУРА

[1] Dasgupta D. Artificial immune systems and their applications. London, Springer, Verlag, 1999.

[2] Dasgupta D., Luis F.N. Immunological computation. Theory and applications. Boca Raton, CRC Press, 2008.

[3] Скобцов Ю.А., Сперанский Д.В. Эволюционные вычисления. М., ИНТУИТ, Лань, 2016.

[4] Castro L.N., von Zuben F.J. Learning and optimization using clonal selection principle. *IEEE Trans. Evol. Comput.*, 2002, vol. 6, no. 3, pp. 239–251.
DOI: https://doi.org/10.1109/TEVC.2002.1011539

[5] Yu X., Gen M. Introduction to evolutionary algorithms. London, Springer, Verlag, 2010.

[6] Forrest S., Perelson A.S., Allen L. Self-nonself discrimination in a computer. *Proc. 1992 Symp. on Security and Privacy*, 1994, pp. 202–212.
DOI: https://doi.org/10.1109/RISP.1994.296580

[7] D'haeseleer P., Forrest S., Helman P. An immunological approach to change detection: algorithms, analysis, and implications. *Proc. IEEE Symp. on Computer Security and Privacy*, 1996, pp. 110–119. DOI: https://doi.org/10.1109/SECPRI.1996.502674

[8] Yang H., Li T., Hu X., et al. A survey of artificial immune system based intrusion detection. *Sc. World J.*, 2014, vol. 2014, art. 156790.
DOI: https://doi.org/10.1155/2014/156790

[9] Dasgupta D., Gonzalez F. An immunity-based technique to characterize intrusion in computer networks. *IEEE Trans. Evol. Comput.*, 2002, vol. 6, no. 3, pp. 281–291.
DOI: https://doi.org/10.1109/TEVC.2002.1011541

[10] Farmer J.D., Packard N.H., Perelson A.S. The immune system, adaptation, and machine learning. *Physica D*, 1986, vol. 22, no. 1-3, pp. 187–204.
DOI: https://doi.org/10.1016/0167-2789(86)90240-X

[11] Jerne N. Towards a network theory of the immune system. *Ann. Immunol.*, 1974, vol. 125C, no. 1-2, pp. 373–389.

[12] Hunt J.E., Cooke D.E. Learning using an artificial immune system. *J. Netw. Comput. Appl.*, 1996, vol. 19, no. 2, pp. 189–212. DOI: https://doi.org/10.1006/jnca.1996.0014

[13] Скобцов Ю.А. Искусственные иммунные системы — основные модели. *Математические методы в технологиях и технике*, 2021, № 2, с. 103–106.
DOI: https://doi.org/10.52348/2712-8873_MMTT_2021_2_103

[14] Скобцов Ю.А. Введение в искусственные иммунные системы. СПб., ГУАП, 2022.

[15] Hofmeyr S.A., Forrest S. Architecture for an artificial immune system. *Envol. Comput.*, 2000, vol. 8, no. 4, pp. 443–473. DOI: https://doi.org/10.1162/106365600568257

[16] Balthrop J., Forrest S., Glickman M.R. Revisting LISYS: parameters and normal behavior. *IEEE World CEC02*, 2002. DOI: https://doi.org/10.1109/CEC.2002.1004387

[17] Balthrop J., Esponda F., Forrest S., et al. Coverage and generalization in artificial immune system. Proc. GECCO, 2002.
URL: http://gpbib.cs.ucl.ac.uk/gecco2002/AAAA243.pdf (дата обращения: 16.05.2022).

[18] Forrest S., Hofmeyr S., Somayaji A. Computer immunology. *Commun. ACM*, 1997, vol. 40, no. 10, pp. 88–96. DOI: https://doi.org/10.1145/262793.262811

[19] Forrest S., Hofmeyr S., Somayaji A., et al. A sense of self for Unix processes. *Proc. IEEE Symp. on Computer Security and Privacy*, 1996.
DOI: https://doi.org/10.1109/SECPRI.1996.502675

[20] Kephart J.O. A biologically inspired immune system for computers. In: Artificial life IV. Cambridge, MIT Press, 1994, pp. 130–139.
DOI: https://doi.org/10.7551/mitpress/1428.003.0017

[21] Kim J., Wilson W.O., Aickelin U., et al. Cooperative automated worm response and detection immune algorithm (CARDINAL) inspired by T-cell immunity and tolerance. In: Artificial immune systems. Springer, Verlag, 2005, pp. 168–181.
DOI: https://doi.org/10.1007/11536444_13

[22] Bradley D.W., Tyrrell A.M. Immunotronics — novel finite-state-machine architectures with built-in self-test using self-nonself differentiation. *IEEE Trans. Evol. Comput.*, 2002, vol. 6, no. 3, pp. 227–238. DOI: https://doi.org/10.1109/TEVC.2002.1011538

Скобцов Юрий Александрович — д-р техн. наук, профессор кафедры компьютерных технологий и программной инженерии ГУАП (Российская Федерация, 190000, Санкт-Петербург, Большая Морская ул., д. 67).

Просьба ссылаться на эту статью следующим образом:

Скобцов Ю.А. Современные иммунологические модели и их приложения. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2022, № 3 (140), с. 61–77.
DOI: https://doi.org/10.18698/0236-3933-2022-3-61-77

MODERN IMMUNOLOGICAL MODELS AND THEIR APPLICATIONS

Yu.A. Skobtsov ya_skobtsov@list.ru

SUAI, St. Petersburg, Russian Federation

Abstract

The paper considers main models and algorithms of artificial immune systems, which are related to the evolutionary computation paradigm and used to search for potential solutions, each of which is represented by an artificial lymphocyte. Same as an individual in evolutionary computation, an artificial lymphocyte is most often encoded by a binary string or a vector of real numbers. As far as the main models of artificial immune systems are concerned, the clonal selection algorithm is close to the evolutionary strategy of evolutionary computing, though it uses more powerful mutation operators and is applied mainly to solve numerical and combinatorial optimisation problems. The negative

Keywords

Artificial immune systems, clonal selection, negative selection, idiopathic network, computer security

selection algorithm is based on the “friend or foe” recognition principle found in the immune system and is most popular in applications. The paper presents two aspects of the algorithm: 1) the basic concept, that is, expanding the set of “friend” cells; 2) the goal, which is to learn to distinguish between “friend” and “foe” cells, while only “friend” cell samples are available. We consider continuous and discrete network models representing regulated networks of molecules and cells. We note the advantages and disadvantages of these models and their application in the field of computer security, robotics, fraud and malfunction detection, data mining, text analysis, image recognition, bioinformatics, games, planning, etc.

Received 27.05.2022
Accepted 14.06.2022

REFERENCES

[1] Dasgupta D. Artificial immune systems and their applications. London, Springer, Verlag, 1999.

[2] Dasgupta D., Luis F.N. Immunological computation. Theory and applications. Boca Raton, CRC Press, 2008.

[3] Skobtsov Yu.A., Speranskiy D.V. Evolyutsionnye vychisleniya [Evolutionary computation]. Moscow, INTUIT, Lan Publ., 2016.

[4] Castro L.N., von Zuben F.J. Learning and optimization using clonal selection principle. *IEEE Trans. Evol. Comput*., 2002, vol. 6, no. 3, pp. 239–251.
DOI: https://doi.org/10.1109/TEVC.2002.1011539

[5] Yu X., Gen M. Introduction to evolutionary algorithms. London, Springer, Verlag, 2010.

[6] Forrest S., Perelson A.S., Allen L. Self-nonself discrimination in a computer. *Proc. IEEE Symp. on Security and Privac*y, 1994, pp. 202–212.
DOI: https://doi.org/10.1109/RISP.1994.296580

[7] D’haeseleer P., Forrest S., Helman P. An immunological approach to change detection: algorithms, analysis, and implications. *Proc. IEEE Symp. on Computer Security and Privacy*, 1996, pp. 110–119. DOI: https://doi.org/10.1109/SECPRI.1996.502674

[8] Yang H., Li T., Hu X., et al. A survey of artificial immune system based intrusion detection. *Sc. World J*., 2014, vol. 2014, art. 156790.
DOI: https://doi.org/10.1155/2014/156790

[9] Dasgupta D., Gonzalez F. An immunity-based technique to characterize intrusion in computer networks. *IEEE Trans. Evol. Comput*., 2002, vol. 6, no. 3, pp. 281–291.
DOI: https://doi.org/10.1109/TEVC.2002.1011541

[10] Farmer J.D., Packard N.H., Perelson A.S. The immune system, adaptation, and machine learning. *Physica D*, 1986, vol. 22, no. 1-3, pp. 187–204.
DOI: https://doi.org/10.1016/0167-2789(86)90240-X

[11] Jerne N. Towards a network theory of the immune system. *Ann. Immunol*., 1974, vol. 125C, no. 1-2, pp. 373–389.

[12] Hunt J.E., Cooke D.E. Learning using an artificial immune system. *J. Netw. Comput. Appl*., 1996, vol. 19, no. 2, pp. 189–212. DOI: https://doi.org/10.1006/jnca.1996.0014

[13] Skobtsov Yu.A. Artificial immune systems — basic models. *Mathematical Methods in Technologies and Technics*, 2021, no. 2, pp. 103–106 (in Russ.).
DOI: https://doi.org/10.52348/2712-8873_MMTT_2021_2_103

[14] Skobtsov Yu.A. Vvedenie v iskusstvennye immunnye sistemy [Introduction to artificial immune systems]. St. Petersburg, GUAP Publ., 2022.

[15] Hofmeyr S.A., Forrest S. Architecture for an artificial immune system. *Envol. Comput*., 2000, vol. 8, no. 4, pp. 443–473. DOI: https://doi.org/10.1162/106365600568257

[16] Balthrop J., Forrest S., Glickman M.R. Revisting LISYS: parameters and normal behavior. *IEEE World CEC02*, 2002. DOI: https://doi.org/10.1109/CEC.2002.1004387

[17] Balthrop J., Esponda F., Forrest S., et al. Coverage and generalization in artificial immune system. *Proc. GECCO*, 2002.
Available at: http://gpbib.cs.ucl.ac.uk/gecco2002/AAAA243.pdf (accessed: 16.05.2022).

[18] Forrest S., Hofmeyr S., Somayaji A. Computer immunology. *Commun. ACM*, 1997, vol. 40, no. 10, pp. 88–96. DOI: https://doi.org/10.1145/262793.262811

[19] Forrest S., Hofmeyr S., Somayaji A., et al. A sense of self for Unix processes. *Proc. IEEE Symp. on Computer Security and Privacy*, 1996.
DOI: https://doi.org/10.1109/SECPRI.1996.502675

[20] Kephart J.O. A biologically inspired immune system for computers. In: Artificial life IV. Cambridge, MIT Press, 1994, pp. 130–139.
DOI: https://doi.org/10.7551/mitpress/1428.003.0017

[21] Kim J., Wilson W.O., Aickelin U., et al. Cooperative automated worm response and detection immune algorithm (CARDINAL) inspired by T-cell immunity and tolerance. In: Artificial immune systems. Springer, Verlag, 2005, pp. 168–181.
DOI: https://doi.org/10.1007/11536444_13

[22] Bradley D.W., Tyrrell A.M. Immunotronics — novel finite-state-machine architectures with built-in self-test using self-nonself differentiation. *IEEE Trans. Evol. Comput*., 2002, vol. 6, no. 3, pp. 227–238. DOI: https://doi.org/10.1109/TEVC.2002.1011538

Skobtsov Yu.A. — Dr. Sc. (Eng.), Professor, Department of Computer Technologies and Software Engineering, SUAI (Bolshaya Morskaya ul. 67, St. Petersburg, 190000 Russian Federation).

Please cite this article in English as:

Skobtsov Yu.A. Modern immunological models and their applications. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2022, no. 3 (140), pp. 61–77 (in Russ.). DOI: https://doi.org/10.18698/0236-3933-2022-3-61-77