УДК 004.8

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

А. В. Селеменев, И. Ф. Астахова, Е. В. Трофименко

Воронежский государственный университет

Поступила в редакцию 07.05.2019 г.

Аннотация. Исследование защиты компьютерных систем с помощью искусственных иммунных систем (ИИС) – это относительно новое направление применения искусственного интеллекта к решению технических задач. Для построения систем обнаружения аномалий могут использоваться различные технологии. В последние годы большое внимание уделяется изучению методов биологического моделирования искусственного интеллекта, таких как искусственные нейронные сети и ИИС. Данные методы являются одними из самых перспективных подходов к решению задач обнаружения аномалий, т. к. они работают максимально приближенно к надежным биологическим иммунным системам человека.

В статье рассматривается решение задачи обнаружения вредоносной информации при помощи алгоритма отрицательного отбора, активно использующегося в искусственных иммунных системах. **Отрицательный отбор** в иммунной системе используется для распознавания чужеродных антигенов путем удаления тех клеток (антител), которые реагируют на собственные антигены. Этот процесс называется распознаванием «свой-чужой». В статье представлен модифицированный алгоритм отрицательного отбора и проведен вычислительный эксперимент с иммунной системой, обнаруживающей сетевые вторжения. Вычислительный эксперимент, демонстрирующий ответную защитную реакцию системы при обнаружении аномального объекта. На конкретном примере рассмотрено применение алгоритма отрицательного отбора.

Ключевые слова: искусственная иммунная система, алгоритм отрицательного отбора, аффинитет, антиген, иммунная память, компьютерная система, защита компьютерной сети.

ВВЕДЕНИЕ

Исследование защиты компьютерных систем с помощью искусственных иммунных систем (ИИС) – это относительно новое направление применения искусственного интеллекта к решению технических задач. Проблема обнаружения изменения свойств или аномалий в поведении объектов может быть сформулирована как задача поиска недопустимых отклонений технических характеристик исследуемой системы. Данная задача может быть решена одним из методов иммунных систем, например, основанным на механизмах отрицательного отбора. **Отрицательный отбор** в иммунной системе используется для распознавания чужеродных антигенов путем удаления тех клеток (антител), которые реагируют на собственные антигены. Этот процесс называется распознаванием «свой-чужой». В статье представлен модифицированный алгоритм отрицательного отбора и проведен вычислительный эксперимент с иммунной системой, обнаруживающей сетевые вторжения [5].

На данный момент систем обнаружения аномалий как самостоятельных продуктов практически не существует, но распространены системы обнаружения вторжений [1], основанные на анализе сигнатур, которые обнаруживают аномалии, связанные с атаками

и вторжениями. Однако сигнатурный метод обладает следующими недостатками:

• невозможность обнаруживать новые, не встречавшиеся ранее несанкционированные воздействия;

• неустойчивость к модификациям уже известных атак;

• неспособность определять распределенные во времени атаки и аномалии [2].

Помимо этого, большинство систем, использующих сигнатурный метод, например RealSecure и NetRanger, являются дорогостоящими продуктами. Среди бесплатных систем обнаружения вторжений, наиболее часто применяемых для защиты сетей передачи данных, можно выделить только систему Snort, но и для этой системы актуальные базы сигнатур являются достаточно дорогими для обыкновенных пользователей. Все эти системы хранят локальные базы данных известных определений компьютерных вирусов. В приведенных программных средствах принятие решения об отнесении неизвестного образца к одному или другому классу осуществляется лишь по окончанию всего цикла сопоставления образцов, что во многих случаях может оказаться уже запоздалой реакцией.

Для построения систем обнаружения аномалий могут использоваться различные технологии. В последние годы большое внимание уделяется изучению методов биологического моделирования искусственного интеллекта, таких как искусственные нейронные сети и ИИС. Данные методы являются одними из самых перспективных подходов к решению задач обнаружения аномалий, т. к. они работают максимально приближенно к надежным биологическим иммунным системам человека. На основе моделей функционирования иммунных систем позвоночных было разработано три класса алгоритмов ИИС: алгоритмы негативного отбора, иммунные сети и алгоритмы клонального отбора [3, 4]. Алгоритмы клонального отбора применяются, в основном, для решения задач оптимизации и поэтому они не рассматриваются в данной работе [4]. ИИС во многом схожи с эволюционными алгоритмами (ЭА), отличаясь от них, в первую очередь, операторами мутации, позволяющими с большей вероятностью получать решения, сильно отклоняющиеся от исходных. Такие операторы мутации называют глобальными. Действие, выполняемое оператором мутации, в ИИС часто зависит от значения функции принадлежности (ФП) мутируемой особи. Это объясняет, почему в начале процесса оптимизации алгоритмы ИИС более эффективны, чем ЭА. Но также это замедляет поиск окончательного решения, так как локальные мутации маловероятны.

Для решения задачи обнаружения аномалий в поступающей на сервер из компьютерной сети информации используется несколько методов искусственных иммунных систем: правило частичного совпадения и отрицательный отбор. Согласно правилу частичного совпадения две сравнивающиеся строки считаются совпадающими, если они находятся друг от друга на расстоянии, не превышающем некоторого значения, рассчитаного с помощью определенных метрик (например, Евклидовой метрики [6]). Две строки совпадают тогда и только тогда, когда они идентичны в определенном числе смежных позиций. Путем сопоставления постоянно поступающих из сети бинарных данных обнаруживаются несовпадения байтов в IP пакетах, которые рассматриваются как аномалия в поведении контролируемой системы. Основное преимущество данного алгоритма состоит в способности обнаруживать новые аномальные изменения, а не искать их среди заранее известного набора заранее подобранных наборов отклонений.

Цель работы – разработка системы обнаружения аномалий, обладающей способностью адаптации к изменениям поведения вычислительной системы с низким числом ложных срабатываний, с использованием методов искусственных иммунных систем.

МАТЕРИАЛЫ И МЕТОДЫ

Алгоритм функционирования ИИС можно представить следующим образом:

1. Генерация собственного набора антигенов.

2. Создание искусственных лимфоцитов на основе собственного набора антигенов с

признаками, определяющими поколение и степень возбуждения антитела. Каждый лимфоцит также имеет несколько антител, которые, по сути, являются детекторами.

3. Отправка в систему чужеродного случайного набора антигенов.

4. Обнаружение антигенов лимфоцитами, что повышает степень возбуждения антитела. При превышении порога возбуждения антитела испускается сигнал об обнаружении аномалии.

5. Увеличивается счетчик поколения для лимфоцита. Осуществляется отбор в текущей популяции антител, имеющих наилучшие показатели аффинитета и получение некоторого количества их копий (клонирование).

6. Происходит мутация клонов антител, заключающаяся во внесении случайным образом изменений в их структуру.

7. Вычисление аффинитета клонов антител.

8. Формирование новой популяции путем присоединения клонов антител к текущей популяции. Определение текущего решения – антитела с наилучшим показателем аффинитета.

9. Удаление некоторой части антител с наихудшими показателями аффинитета.

10. Генерация новых случайно сформированных антител и их присоединение к популяции до восстановления ее численности N.

11. Условием окончания алгоритма является стабилизация популяции на протяжении некоторого количества циклов. Если условие выполнено, то решением является антитело с наилучшим показателем аффинитета, если не выполнено, то происходит переход к шагу 3.

Рассмотрим этот алгоритм применительно к разрабатываемой системе (рис. 1).

1. Модель для построения ИИС состоит из набора шести обычных шаблонов (которые не должны быть частью предполагаемой сетевой атаки), представляющих собой описание сетевых пакетов TCP/IP в двоичной форме. Это называется собственным набором антигенов в терминологии ИИС. В реальной системе такой набор будет содержать десятки или сотни тысяч шаблонов, и каждый шаблон будет намного больше чем 12 бит (обычно 48–256 бит заголовка запроса характеризуют и позволяют классифицировать входящий в запрос IP пакет), но в связи с ограничениями вычислительных мощностей для эксперимента используются шаблоны по 12 бит.

2. На основе этих шаблонов создается три искусственных лимфоцита. Каждый лимфоцит имеет смоделированное антитело, которое имеет четыре бита, поколение и степень возбуждения. Поля антитела, по существу, являются детектором. Лимфоциты создаются таким образом, что ни один из них не обнаруживает никаких шаблонов в собственном наборе. Каждый лимфоцит имеет три последовательных бита, равных 0 или 1, но ни один из шаблонов в собственном наборе не имеет трех последовательно равных битовых значений.

3. Антигены обнаруживаются лимфоцитами. Каждый лимфоцит имеет несколько антител, которые можно рассматривать как детекторы. Каждое антитело специфично для конкретного антигена. Как правило, поскольку соответствие антитело-антиген является только приблизительным, лимфоцит не будет вызывать реакцию, когда одно антитело обнаруживает один антиген. Только после того, как несколько антител обнаружат соответствующие антигены, лимфоцит будет простимулирован и система отреагирует какой-либо реакцией. Аффинитет – это степень соответствия, определяющая прочность связи между антителом и антигеном. Чем больше соответствие антитела – антигену, тем больше аффинитет. В иммунных сетях различают два вида аффинитета: 1) степень различия – аффинитет связи антиген-антитело (Ag-Ab); 2) степень соответствия – аффинитет связи антитело-антитело (Ab-Ab).

С точки зрения системы обнаружения вторжений антигены соответствуют сетевым пакетам TCP/IP, тело которых содержит какие-либо данные, характеризующие входящий шаблон как вредоносный. Собственные антигены соответствуют безопасным сетевым запросам. Антитело соответствует побитовой схеме, которая приблизительно соответствует неизвестному, потенциально опасному шаблону. Лимфоцит представляет собой два или более антител/детекторов. Апоптоз моделируется с использованием теории, называемой клонально-селективной теорией [7]. Также

Рис. 1. Блок-схема работы алгоритма ИИС для обнаружения аномалий

эту теорию еще называют естественным отбором [8].

4. Разработка и анализ методов, объединяющих различные операторы мутации в одном алгоритме, является развивающейся областью исследований ИИС. Одними из таких методов являются меметические алгоритмы, использующие один или несколько алгоритмов локального поиска для небольших локальных улучшений особей в процессе оптимизации мутации, производимой эволюционным алгоритмом [9]. Выбор операторов локального поиска может быть произведен либо на каждой итерации мутации популяции (такой подход называется итерированным локальным поиском [10]), либо адаптивно из заданного набора операторов [11]. Другим методом адаптивного выбора операторов мутации является обучение с подкреплением [12, 13]. В рамках этого метода сущность, называемая агентом обучения, на каждой итерации алгоритма оптимизации согласно некоторой стратегии выбирает действие – один из возможных операторов мутации – и сообщает его среде (в качестве которой выступает эволюционный алгоритм). За это действие агент получает от среды награду и, в зависимости от ее величины, обновляет свою стратегию. Награда основана на росте функции приспособленности (ФП), следовательно, агент учится выбирать операторы, которые позволяют быстрее найти решение с высоким значением ФП [14–17].

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Система обнаружения сетевых вторжений разделяется на несколько модулей: модуль веб-сервера, модуль журналирования сетевого трафика, модуль обнаружения аномалий, модуль оповещения, модуль реагирования на отрицательное воздействие. Структура системы обнаружения сетевых вторжений представлена на рис. 2.

Модуль веб-сервера представляет собой классический HTTP сервер, который имеет возможность принимать основные виды HTTP запросов. Данный модуль является точкой входа в приложение.

Модуль журналирования сетевого трафика является плагином для веб-сервера и имеет возможность извлекать и журналировать информацию о субъектах, осуществляющих запросы на основе данных IP пакета. В журнал записывается такая информация как IP адрес, название клиентского приложения (user-agent), тело запроса, заголовки запроса, время выполнения запроса.

Рис. 2. Логическое разделение на программные модули

Модуль обнаружения аномалий состоит из двух блоков. Блок обнаружения аномалий содержит подпрограмму обнаружения вредоносных запросов на основе алгоритмов ИИС. Когда обнаруживается вредоносный запрос, он вносится в список заблокированных запросов. Блок формирования иммунной памяти содержит список заблокированных адресов и доверенный список исключений.

Модуль оповещения вызывается из модуля обнаружения аномалий, основная его задача уведомить заинтересованные объекты об обнаружении аномалии в сетевых запросах, поступающих на веб-сервер.

Модуль реагирования на отрицательное воздействие осуществляет запись атакующих систему IP адресов и защитный сетевой экран с целью не допустить дальнейшее проникновение запросов на веб-сервер с нежелательных IP адресов.

После инициализации системы программа начинает симуляцию работы веб-сервера, на который поступают по шесть запросов в каждой итерации, таким образом алгоритм начинает работу с шестью шаблонами ввода. Первый шаблон обнаруживается лимфоцитами 0 и 1, но поскольку у каждого лимфоцита есть порог активации, лимфоцит не вызывает никакой реакции. На втором вводе лимфоцит 0 обнаруживает другой подозрительный шаблон, но еще не достигший порога. На третьем вводе лимфоцит 0 обнаруживает третий подозрительный входной шаблон и выдает предупреждение.

Одной из ключевых частей любой ИИС является процедура, которая определяет, обнаруживает ли шаблон антиген. Требование точного соответствия антитела антигену невозможно (и не имитирует реальное поведение антигена). Ранние работы над ИИС использовали метод, называемый правилом частичного совпадения, в котором как антиген, так и исходный шаблон имеют одинаковое количество бит и обнаружение происходит, когда антиген и шаблон совпадают в r последовательных символах. Более поздние исследования показали, что лучшим алгоритмом обнаружения является использование правила частичного совпадения. Использование цепочек битов схоже с использованием последовательных битов, за исключением того, что детектор антигена меньше, чем шаблон для проверки, и обнаружение происходит, когда антиген соответствует некоторому подмножеству шаблона. Например, если антиген равен 110, а шаблон 000**110**111, то антиген обнаруживает образец, начинающийся с индекса 3.

Метод частичного совпадения – это почти то же самое, что и функция поиска подстроки. Единственное различие заключается в том, что последовательности, совпадающие с битами и подстрокой, соответствуют символам 0 и 1.

В рассмотренном выше примере подход к правилу частичного совпадения состоит в том, чтобы исследовать шаблон, начинающийся с индекса 0, затем по индексу 1, затем по 2 и так далее. Однако в большинстве случаев этот подход работает очень медленно. Существует несколько сложных алгоритмов поиска подстрок, которые обрабатывают меньшую строку детектора для создания массива ассоциаций или таблицы. Эта таблица поиска может использоваться для быстрого прохода вперед при поиске несоответствий,

тем самым значительно повышается производительность программы. В ситуациях, когда небольшая строка детектора многократно используется для проверки разных шаблонов – как при обнаружении вторжения в ИИС, время и память, необходимые для создания таблицы поиска, – это наименьшая цена, которая платится за значительно более высокую производительность.

Метод обнаружения вхождения строк для лимфоцитов использует алгоритм подстроки Кнута – Морриса – Пратта [3], применяемый к битовым массивам. Это эффективный алгоритм, осуществляющий поиск подстроки в строке. Время работы алгоритма линейно зависит от объёма входных данных, то есть разработать асимптотически более эффективный алгоритм невозможно. Метод обнаружения принимает шаблон ввода, такой как 000110111, и возвращает истинное значение, если антиген текущего объекта, такой как 101, соответствует шаблону, поданному на вход. Метод обнаружения предполагает существование таблицы поиска.

ЗАКЛЮЧЕНИЕ

Спроектирована система обнаружения сетевых вторжений с применением методов ИИС. Данный подход хорошо применим к такой разновидности компьютерных атак, как распределенная атака с целью вызвать отказ в обслуживании [4].

Важно отметить, что использование ИИС не является единственным решением для обнаружения вторжений в компьютерную сеть. Этот подход должен быть частью многоуровневой защиты, которая включает в себя как традиционное антивирусное программное обеспечение, так и решения по обеспечению безопасности на аппаратном уровне.

СПИСОК ЛИТЕРАТУРЫ

1. *Гончаров, В. А.* Метод обнаружения сетевых атак, основанный на кластерном анализе взаимодействия узлов вычислительной сети / В. А. Гончаров, В. Н. Пржегорлинский // Вестник Рязанского государственного радиотехнического университета. – 2011. – № 36. – С. 3–10.

2. *Сухов, В. Е.* Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов / В. Е. Сухов // Вестник РГРТУ. – 2015. – № 54, Ч. 1. – С. 84.

3. *Knuth, D.* Fast pattern matching in strings / D. Knuth, J. H. Morris, Jr, V. Pratt // SIAM Journal on Computing. – 1977. – № 6 (2). – P. 323–350. – DOI:10.1137/0206024.

4. Understanding Denial-of-Service Attacks [Электронный ресурс] // US-CERT. – URL: https://www.us-cert.gov/ncas/tips/ST04-015 (дата обращения 11.12.2018).

5. *Демидова, Л. А.* Исследование влияния основных параметров алгоритма функционирования искусственной иммунной сети на качество кластеризации объектов / Л. А. Демидова, С. Б. Титов // Вестник Рязанского государственного радиотехнического университета. – 2012. – № 40. – С. 54–60.

6. *Howard, A.* Elementary Linear Algebra / A. Howard. – 7th ed. – 1994. – John Wiley & Sons. – P. 170–171.

7. *Burnet, F. M.* Modification of Jerne's theory of antibody production using the concept of clonal selection / F. M. Burnet // A Cancer Journal for Clinicians. – 1976 CA. – № 26 (2). – P. 119–21.

8. Селективные теории образования антител. [Электронный ресурс] // Иммунология. URL: http://imuno.net/59.php (дата обращения 14.12.2018).

9. *Neri, F.* Handbook of Memetic Algorithms / F. Neri, C. Cotta, P. Moscato. – Springer, 2012. – 370 p. – DOI: 10.1007/978-3-642-23247-3.

10. *Sudholt, D.* Memetic algorithms with variable-depth search to overcome local optima / D. Sudholt // Proc. 10th Genetic and Evolutionary Computation Conference. – Atlanta: USA. – 2008. – P. 787–794.

11. *Smith, J. E.* Self-adaptative and coevolving memetic algorithms / J. E. Smith // Studies in Computational Intelligence. – 2012. – V. 379. – P. 167188. – DOI: 10.1007/978-3-642-23247-3_11.

12. *Sutton, R. S.* Reinforcement Learning: An Introduction / R. S. Sutton, A. G. Barto. – Cambridge : MIT Press, 1998. – 344 p.

13. *Buzdalova, A.* Selecting evolutionary operators using reinforcement learning: Initial explorations / A. Buzdalova, V. Kononov, M. Buzdalov // Proc. 16th Genetic and Evolutionary Computation Conference. – Vancouver : Canada, 2014. – P. 1033–1036. – DOI: 10.1145/2598394.2605681.

14. *Ушаков, С. А.* Разработка и исследование алгоритмов решения задач распознавания на основе искусственных иммунных систем: Автореф…дисс… канд. техн. наук. – Воронеж : ВГУ, 2015. – 16 с.

15. *Киселева, Е. И.* Алгоритм использования искусственной иммунной системы для оптимизации целевого компонента информационной образовательной системы / Е. И. Киселева, И. Ф. Астахова // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2017. – № 2. – С. 61–65.

16. *Makoviy, K. A.* Server hardware resources optimization for virtual desktop implementation / K. Makoviya, Yu. Khitskovaa, Ya. Metelkin // Информационные технологии и нанотехнологии: Сб. трудов III Межд. конф. и молодежной школы «ИТНТ-2017». – Самара. – С. 25–27.

17. *Маковий, К. А.* Использование метода гибридных оценок в области информационных технологий / К. А. Маковий, Ю. В. Хицкова, С. В. Герус // Научный вестник. Информационные технологии в строительных, социальных и экономических системах. – 2016. – № 1 (7). – С. 120–124.

Селеменев А. В. – аспирант кафедры МО ЭВМ факультета ПММ, Воронежский государственный университет.
E-mail: andreyjkee@gmail.com

Астахова И. Ф. – д-р техн. наук, профессор, профессор кафедры МО ЭВМ факультета ПММ, Воронежский государственный университет.
E-mail: astachova@list.ru

Трофименко Е. В. – канд. техн. наук, доцент кафедры МО ЭВМ факультета ПММ, Воронежский государственный университет.
E-mail: evtrof@gmail.com

APPLICATION OF ARTIFICIAL IMMUNE SYSTEMS FOR DETECTION OF NETWORK INCLUSIONS

A.V. Selemenev, I.F. Astachova, E.V. Trofimenko

Voronezh State University

Annotation. The study of the protection of computer systems with the help of artificial immune systems (IIS) is a relatively new direction in the application of artificial intelligence to solving technical problems. Various technologies can be used to build anomaly detection systems. In recent years, much attention has been paid to the study of methods of biological modeling of artificial intelligence, such as artificial neural networks and IIS. These methods are one of the most promising approaches to solving problems in the detection of anomalies, because they work as close as possible to reliable biological immune systems of humans.

The article discusses the solution of the problem of detecting malicious information using the negative selection algorithm that is actively used in artificial immune systems. Negative selection in the immune system is used to recognize foreign antigens by removing those cells (antibodies) that respond to their own antigens. This process is called «friend-foe» recognition. The article presents a modified negative selection algorithm and conducted a simulation experiment with the immune system detecting network invasions. A simulation experiment of an attack on a computer

system and demonstrates the response of the system when an abnormal object is detected. For a specific example, a negative selection algorithm is applied. The article is a presentation of the idea of modeling a software system based on the behavior of the human immune system.
Keywords: artificial immune system, negative selection algorithm, antigen, immune memory, computer system, computer network defense.

Selemenev A. V. – post graduate student, Department of applied mathematics, Informatics and Mechanics, Voronezh State University.
E-mail: andreyjkee@gmail.com

Astachova I. F. – doctor technical science, prof., prof. Department of applied mathematics, Informatics and Mechanics, Voronezh State University
E-mail: astachova@list.ru

Trofimenko E. V. – candidate technical science, Department of applied mathematics, Informatics and Mechanics, Voronezh State University
E-mail: evtrof@gmail.com