УДК 004.056 doi: 10.26102/2310-6018/2019.24.1.010

В.И.Васильев, Р.Р.Шамсутдинов

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ МЕХАНИЗМОВ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ

ФБГОУ ВО «Уфимский государственный авиационный технический университет» Уфа, Россия

Статья посвящена проблеме обнаружения сетевых атак, как известных, так и неизвестных ранее. Проанализировано применение различных методов искусственного интеллекта к решению данной проблемы в научной литературе, выявлены преимущества искусственной иммунной системы, проанализированы основные ее механизмы: генерации и негативной селекции искусственных лимфоцитов, их периодического обновления, определения факта их реагирования и клональной селекции среагировавших лимфоцитов; описана разработанная система обнаружения атак на основе искусственной иммунной системы, содержащая подсистему сниффинга, что позволяет ей анализировать реальные данные о сетевых соединениях на уровне хоста. Также был описан набор данных о сетевых соединениях KDD99, с использованием которого проведена оценка эффективности разработанной системы. Проанализирована научная литература, предлагающая способы сжатия исходного множества данных, выявлены недостатки предложенных способов, проведено самостоятельное экспериментальное определение значимых параметров сетевых соединений, содержащихся в наборе данных. Было идентифицировано 13 значимых параметров из 41. Описана предварительная обработка и подготовка анализируемых данных, серия проведенных экспериментов, по результатам которых была определена высокая эффективность разработанной системы в обнаружении неизвестных сетевых атак, обнаружении и классификации известных атак.

Ключевые слова: система обнаружения атак, искусственная иммунная система, KDD99, информационная безопасность, безопасность сети, сетевая атака.

Введение

Современный этап развития информационных технологий обуславливает необходимость обеспечения высокого уровня обнаружения новейших сетевых атак, несущих угрозы интересам организаций в информационной сфере, обеспечению непрерывности бизнеса и безопасности защищаемой законом информации, поскольку в настоящее время появляются все новые, неизвестные ранее угрозы информационной безопасности (ИБ), реализация которых может вызвать простои в работе информационных систем (ИС), нарушить доступность,

конфиденциальность и целостность информации, что может привести к нарушению законодательства, убыткам и банкротству организаций.

Системы обнаружения атак – достойный механизм противодействия сетевым угрозам. Искусственные иммунные системы (ИИС) – системы безопасности, имитирующие работу естественной иммунной системы человека, способны выявлять неизвестные ранее виды угроз, адаптироваться под лучшее обнаружение угроз, подобных каждой выявленной, характеризуются постоянным обновлением иммунитета с сохранением иммунной памяти. Таким образом, система обнаружения атак, основанная на ИИС, характеризуется возможностью выявления известных и неизвестных сетевых атак, способностью к самообучению.

Целью данной работы является тестирование на реальных данных о сетевой активности, разработанной нами ранее в [1] системы обнаружения атак на основе ИИС, способной выявлять как известные, так и неизвестные ранее атаки, эффективность которой была проверена только на тестовых данных. Поскольку реализованная атака является вторжением, в данной статье понятия системы обнаружения атак и системы обнаружения вторжений (СОВ) будем считать эквивалентными.

В решении задачи обнаружения вторжений широко применяются:

- экспертные системы [2];
- искусственные нейронные сети[3, 4];
- нечеткие системы [5, 6];
- генетические алгоритмы [7];
- ИИС [8, 9].

Разработанная СОВ основана на ИИС, поскольку, как представлено в [10, 11], в реальных задачах распознавания иммунокомпьютинг превосходит своих основных конкурентов (искусственные нейронные сети и генетические алгоритмы), как минимум, в 40 раз по быстродействию и в 2 раза по безошибочности распознавания.

Базовый механизм построения СОВ

Иммунная система представляет собой распределенный многоуровневый механизм защиты от чужеродных микроорганизмов, вирусов и патогенов [12]. ИИС, по аналогии с естественной иммунной системой, состоит из множества искусственных лимфоцитов, каждый из которых представляет собой детектор, толерантный к нормальному состоянию контролируемой системы. Реагирование детектора на единицу

анализируемых данных – есть обнаружение аномалии. Каждая единица анализируемых данных – вектор-строка определенной длины, каждый детектор также является вектор-строкой соответствующей длины. Необходимо рассмотреть такое понятие как аффинность – число поэлементно совпадающих значений в двух сравниваемых строках. Факт реакции определяется достижением аффинности заданного порогового значения.

Толерантность детекторов к нормальному состоянию анализируемых данных и друг к другу обеспечивается механизмом негативной селекции. В первую очередь осуществляется сбор строк данных, характеризующих нормальное состояние. Затем случайным образом генерируются детекторы, определяется факт реагирования каждого нового детектора к каждой строке нормальной активности, и к каждому ранее сгенерированному детектору, если новый детектор среагировал хотя бы единожды, то он уничтожается, генерируется новый детектор, иначе, считается, что новый детектор прошел процедуру негативной селекции и сохраняется. На этом этап первичного обучения ИИС завершается.

Таким образом, получается набор детекторов, толерантный к нормальной активности контролируемой системы, способный обнаруживать аномалии. Следует отметить, что каждый детектор должен иметь «срок жизни», по истечении которого детектор заменяется новым, случайно сгенерированным детектором, прошедшим механизм негативной селекции.

Анализ данных осуществляется вычислением аффинности между каждым детектором и каждой анализируемой строкой, при достижении аффинности порогового значения, считается, что обнаружена аномалия.

Как отмечается в [13] и [14], адаптивность искусственного иммунитета обеспечивается другим важным механизмом – клональной селекцией, который заключается в следующем. Если детектор обнаружил аномалию, он копируется заданное количество раз с изменением случайных его элементов новыми случайными значениями, каждый такой клон также подвергается негативной селекции, затем заменяет собой детектор, среагировавший наименьшее число раз. Срок жизни среагировавшего на аномалию детектора должен быть увеличен.

На основе данных механизмов была разработана система обнаружения сетевых атак. Состав модулей и их взаимодействие в разработанной системе представлено на Рисунке 1.

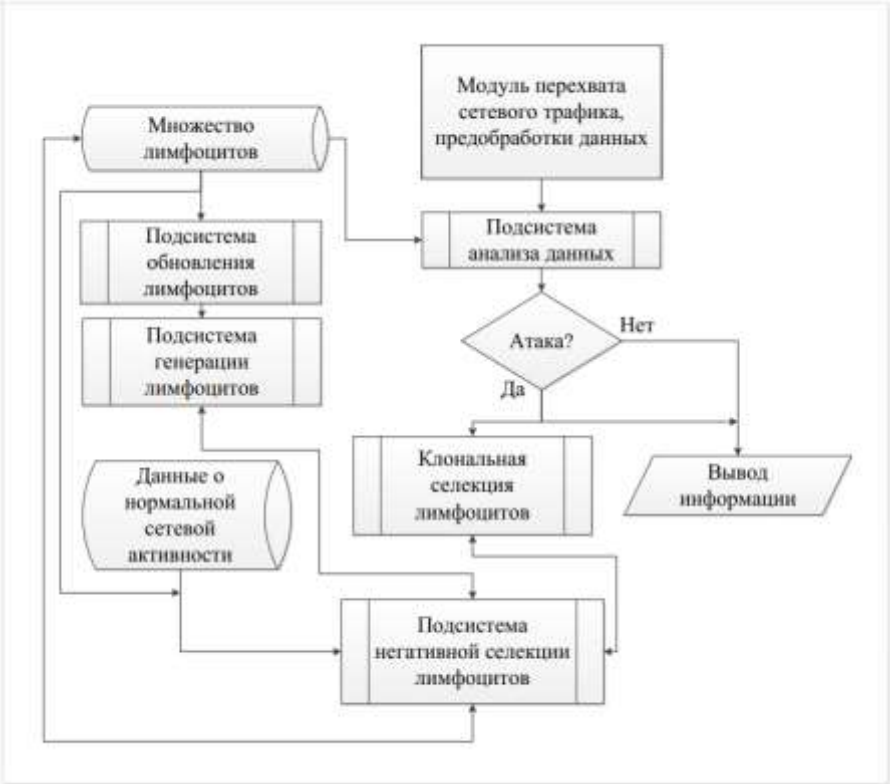

Рисунок 1 – Состав и взаимодействие модулей разработанной системы

Для тестирования эффективности выявления разработанной системой реальных сетевых атак решено использовать KDD Cup 99 Data (KDD 99) [15]. KDD 99 – это набор данных, который был сгенерирован путем эмуляции военного сетевого окружения в 1999 г. Набор данных был создан в военной среде, в которой локальная сеть военно-воздушных сил была подвергнута смоделированным атакам. Он содержит около 4 млн. строк данных о сетевых соединениях, каждая строка содержит 41 параметр. Также дополнительно существует набор данных KDD в объеме 10% от основного набора.

Каждая строка данных о сетевых соединениях содержит 41 параметр, анализ такого массива требует значительных вычислительных ресурсов, в связи с этим необходимо уменьшить длину анализируемого вектора.

Рассмотрим наборы параметров, предлагаемые в научной литературе. В статье [16] можно найти один из наборов. В данном случае для нахождения параметров использовался алгоритм DPSO. Идея алгоритма заключается в решении задачи оптимизации с помощью моделирования поведения популяции частиц в пространстве параметров.

Также набор значимых параметров формируется в статье [17], где используется алгоритм SVDF. Он является разновидностью метода опорных векторов. Сначала исходный набор данных подается на вход классификатора для обучения. Затем для оценки важности параметров используется решающая функция классификатора. Процедура представляет собой следующее:

– вычисляется вес от решающей функции вектора поддержки;
– оценивается важность параметров по абсолютному значению весов.

В статье [18] набор значимых параметров находится с помощью удаления за раз одного параметра, чтобы оценить его и идентифицировать самые важные для обнаружения проникновений. Задачей было получить 5 самых значимых параметров для каждого типа атак.

В [19] по мнению авторов, рассматриваемый подход достигает самой высокой усредненной точности с сокращением размера входных данных в сравнении с другими. В статье [20] предлагаются параметры: logged_in; dst_host_diff_srv_rate; dst_host_same_srv_rate; duration;src_bytes root_shell; count; dst_bytes; dst_host_same_src_port_rate; wrong_fragment; srv_count. В [12] предлагается сжатие множества KDD 99 с использованием сингулярного разложения матриц. Данное сжатие эффективно и поддерживает полное восстановление с незначительной погрешностью.

Однако параметры, предлагаемые в [16-19] отличаются для каждого вида атаки. По параметрам, предлагаемым в [20], обнаружить угрозы не удалось. Сжатие с использованием сингулярного разложения матриц позволяет проводить классификацию единовременно сжатых данных, однако не позволяет анализировать все новые и новые строки сетевой активности. В связи с этим было принято решение о необходимости самостоятельного выделения значимых параметров сетевых соединений KDD 99.

Анализ 4 млн. строк даже с целью выбора значимых параметров требует значительных вычислительных ресурсов, поэтому было принято решение использовать дополнительный набор из 10% данных сетевых соединений KDD 99.

Было осуществлено приведение значений параметров к виду, удобному для анализа:

– лингвистические данные были кодированы целыми неотрицательными числами, максимальное полученное число – 65;

– исходные десятичные дроби, округленные до сотых, не превышающие единицу, были умножены на 100;

– целочисленные неотрицательные значения, не превышающие 255, были оставлены без изменений, не превышающие 511 были разделены на 2 с округлением до целых;

– целочисленные неотрицательные параметры, максимальные значения которых достигают миллионов, были сжаты следующим образом. Для каждого параметра было выбрано пороговое значение P, близкое к соответствующему максимальному, содержащемуся в наборе KDD 99. Если исходное значение строго равно нулю, то сжатое значение строго равно нулю. Если исходное значение больше нуля и не превышает порогового, то сжатие осуществляется равномерно так, чтобы сжатое значение лежало в диапазоне [1; 254]. Если исходное значение превышает пороговое, то сжатое равно 255.

Была написана программа, загружающая в двумерные массивы строки и их элементы для аномальной и нормальной активности. Каждая строка аномальной активности сравнивается поэлементно с каждой строкой нормальной активности для нахождения максимального числа поэлементного совпадения для A_j со строками множества N. При нахождении такой пары строк каждый совпадающий элемент заменяется единицей, не совпадающий – нулем, и полученная строка записывается в отдельный файл, на основе которого был подсчитан процент совпадений по каждому параметру между строками нормальной и аномальной активности. Полученные результаты ранжированы по наименьшему проценту совпадений.

Целесообразнее выбирать параметры с минимальным числом совпадений. Решено провести серию вычислительных экспериментов сначала по первым 16 ранжированным параметрам, затем постепенно уменьшать число параметров, а в случае неудовлетворительной эффективности анализа по 16 параметрам постепенно увеличивать их количество.

Исходное множество KDD 99 было предварительно обработано и разделено на данные о нормальной сетевой активности и данные об атаках, затем каждое из полученных множеств было разделено еще раз на данные для обучения и данные для оценки эффективности. Для каждого набора параметров лимфоциты генерировались заново с соответствующей длинной детектирующей строки.

ИИС нацелена на выявление всего чужеродного, в том числе, совершенно неизвестных атак, однако нелишним было бы добавить

возможность классификации известных атак. Для этого алгоритмом генерации в первую очередь создавались формальные лимфоциты с детектирующими строками, идентичными строкам аномальной активности обучающих данных.

Было создано около 200 000 таких лимфоцитов, затем пока не достигнуто принятое количество лимфоцитов в 500 000 единиц, алгоритмом генерации создается лимфоцит со случайным значением детектирующей строки, после чего вычисляется аффинность между лимфоцитом и каждой строкой из множества нормальной активности, а также сгенерированными ранее лимфоцитами. Если хотя бы одно значение аффинности достигает порогового, принятого на единицу меньшим числа параметров, то лимфоцит отбрасывается и генерируется новый, иначе, лимфоцит добавляется во множество детекторов, которые хранятся в постоянной памяти в бинарном файле.

Для тестирования эффективности выявления системой реальных атак был запущен анализ подготовленных данных. Анализ проводился несколько раз, поскольку системе необходимо обучиться на анализируемых данных. Было проведено две серии экспериментов:

– для оценки эффективности классификации известных атак анализ осуществлялся с использованием лимфоцитов, как со случайными значениями детектирующей строки, так и с полностью соответствующими обучающим строкам данных атак (произведено 10 итераций анализа);

– для оценки эффективности обнаружения неизвестных атак анализ осуществлялся с использованием лимфоцитов со случайными значениями детектирующей строки, обученных только толерантности к нормальной активности, для них каждая атака, содержащаяся в KDD 99, является неизвестной (произведено 19 итераций анализа).

Результаты вычислительных экспериментов

По итогам анализа первых 16 параметров, эффективность системы оказалась высокой, в связи с этим число анализируемых параметров постепенно уменьшалось. Ошибки первого рода по итогам каждой итерации анализа с использованием лимфоцитов, не только со случайно сгенерированными детектирующими значениями, но и с обученными классификации неизвестных атак сведены в Таблице 1.

Таблица 1 – Процент ошибок первого рода

Число парамет-ров / № итерации	8	9	10	11	12	13	14	16
1	0,12%	0,16%	0,19%	0,19%	0,14%	0,15%	0,13%	0,02%
2	0,12%	0,11%	0,14%	0,14%	0,13%	0,11%	0,11%	0,014%
3	0,12%	0,11%	0,11%	0,10%	0,10%	0,10%	0,10%	0,013%
4	0,12%	0,11%	0,11%	0,10%	0,10%	0,08%	0,08%	0,012%
5	0,12%	0,11%	0,11%	0,10%	0,10%	0,05%	0,05%	0,011%
6	0,12%	0,11%	0,11%	0,10%	0,10%	0,04%	0,04%	0,010%
7	0,12%	0,11%	0,11%	0,10%	0,10%	0,04%	0,03%	0,009%
8	0,12%	0,11%	0,11%	0,10%	0,10%	0,03%	0,03%	0,008%
9	0,12%	0,11%	0,11%	0,10%	0,10%	0,02%	0,015%	0,007%
10	0,12%	0,11%	0,11%	0,10%	0,10%	0,013%	0,013%	0,006%

По данным Таблицы 1, для числа параметров менее 13 определяется некоторый предел снижения процента ошибок 1-го рода, предельные значения выделены цветом, однако при числе параметров от 13 и более – процент ошибок 1-го рода продолжает снижаться от итерации к итерации.

Ошибки второго рода по итогам каждой итерации анализа с использованием лимфоцитов, не только со случайно сгенерированными детектирующими значениями, но и с обученными классификации неизвестных атак сведены в Таблице 2.

При выборе числа параметров менее 13 аналогично наблюдается предел снижения ошибок 2-го рода. Логичным было бы предположить, что значимыми являются не выбранные 13 параметров, а 13-ый параметр, однако процент совпадений между строками нормальной и аномальной активности по нему составляет 99,3%.

Таким образом, по выбранным 13 параметрам (23; 24; 3; 30; 33; 29; 34; 35; 32; 4; 36; 40; 5) система демонстрирует высокий уровень обнаружения известных атак с их классификацией.

Результаты анализа с использованием лимфоцитов со случайно сгенерированными детектирующими значениями, для которых каждая атака из KDD 99 является неизвестной, представлены на Рисунке 2.

Таблица 2 – Процент ошибок второго рода

Число параметров / № итерации	8	9	10	11	12	13	14	16
1	3,44%	3,42%	4,96%	4,99%	6,13%	5,80%	5,80%	5,93%
2	2,94%	2,80%	3,40%	3,45%	4,31%	4,16%	4,09%	4,29%
3	2,94%	2,80%	2,40%	2,37%	2,52%	1,75%	1,69%	2,12%
4	2,94%	2,80%	2,40%	2,37%	1,73%	1,46%	1,39%	1,46%
5	2,94%	2,80%	2,40%	2,37%	1,73%	0,73%	0,70%	0,63%
6	2,94%	2,80%	2,40%	2,37%	1,73%	0,68%	0,67%	0,56%
7	2,94%	2,80%	2,40%	2,37%	1,73%	0,56%	0,55%	0,52%
8	2,94%	2,80%	2,40%	2,37%	1,73%	0,50%	0,47%	0,43%
9	2,94%	2,80%	2,40%	2,37%	1,73%	0,36%	0,36%	0,34%
10	2,94%	2,80%	2,40%	2,37%	1,73%	0,28%	0,26%	0,21%

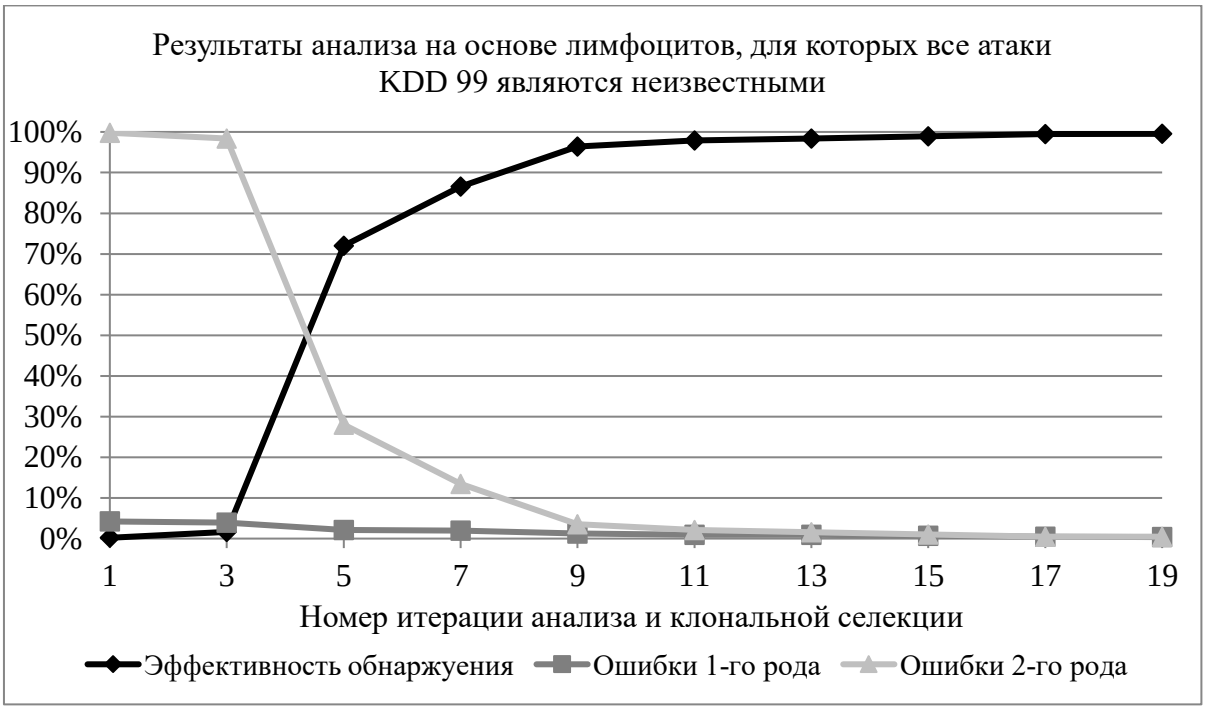

Рисунок 2 – Результаты анализа на основе лимфоцитов, для которых все атаки KDD 99 являются неизвестными

Как видно из Рисунка 2, система демонстрирует высокую эффективность обнаружения неизвестных для нее атак. По результатам 19 итерации анализа эффективность обнаружения превысила 99%, уровень ошибок 1 и 2 рода не превышает 0,5%.

В работах [21-23] подробно описаны преимущества распределенных IDS на основе механизмов иммунной системы, главное из которых – это тот факт, что при обнаружении атаки и адаптации к лучшему обнаружению подобных атак одним хостом, аналогичным образом адаптируются к подобным атакам все другие хосты системы. В будущем планируется доработка системы и ее тестирование в качестве распределённой системы обнаружения атак на реальных данных.

Заключение

Таким образом, система способна с высокой эффективностью обнаруживать и классифицировать известные ей атаки, выявлять неизвестные, используя для анализа значимые параметры сетевых соединений, содержащихся в KDD99, то есть параметры: 3; 4; 5; 23; 24; 29; 30; 32; 33; 34; 35; 36; 40. Использование меньшего количества параметров не рекомендуется ввиду наличия предела снижения ошибок первого и второго рода, использование же 13 параметров позволяет снижать процент ошибок от итерации к итерации. Использование большего числа параметров требует бóльших временных затрат на анализ.

Работа выполнена при поддержке гранта РФФИ №17-48-020095.

ЛИТЕРАТУРА

1. Васильев В. И., Шамсутдинов Р. Р. Распределенная система обнаружения атак на основе механизмов иммунной системы // Труды VI Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений» (с приглашением зарубежных ученых) Т. 1, Уфа, 28-31 мая, 2018. С. 237-244.
2. Корнев П. А., Пылькин А. Н., Свиридов А. Ю. Применение инструментария искусственного интеллекта в системах обнаружения вторжений в вычислительные сети // Современные проблемы науки и образования. – № 6. – 2014.– С. 135-143.
3. Браницкий А. А., Котенко А. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. – № 2 (45). – Санкт-Петербург, 2016. – С. 207-244.

4. Жигулин П. В., Подворчан Д. Э. Анализ сетевого трафика с помощью нейронных сетей // Электронные средства и системы управления. – № 2. – 2013. – С. 44-48.
5. Shanmugavadivu R., Nagarajan N. Network intrusion detection system using fuzzy logic // Indian Journal of Computer Science and Engineering [Electronic resource]. URL: http://www.ijcse.com/docs/IJCSE11-02-01-034.pdf (accessed 29.03.2018).
6. Слеповичев И. И., Ирматов П. В., Комарова М. С., Бежин А. А. Обнаружение DDoS атак нечеткой нейронной сетью // Известия. Саратовского университета. Серия Математика. Механика. Информатика. – № 9. – 2009. – С. 84-89.
7. Goyal A., Kumar C. GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System // Northwestern University [Electronic resource]. URL: http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf (accessed 29.03.2018).
8. Al-Enezi J.R., Abbod M.F., Alsharhan S. Artificial Immune Systems – Models, Algorithms and Applications // IJRRAS. – Vol. 2. – № 3. – 2010. – pp. 118-131.
9. Bachmayer S. Artificial Immune Systems // Tietojenkäsittelytieteen laitos. [Electronic resource]. URL: https://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/bachmayer.pdf (accessed 01.03.2018).
10. Tarakanov A.O., Tarakanov Y.A. A comparison of immune and genetic algorithms for two real-life tasks of pattern recognition // Int. J. of Unconventional Computing. – Vol. 1.4. – 2004. – pp. 357-374.
11. Tarakanov A.O., Tarakanov Y.A. A comparison of immune and neural computing for two real-life tasks of pattern recognition // International Conference on Artificial Immune Systems. – Catania, 2004. – pp. 236-249.
12. Васильев В. И., Котов В. Д. Система обнаружения сетевых вторжений на основе механизмов иммунной модели // Известия ЮФУ. Технические науки. – № 12(125). – Таганрог, 2011. – С. 180-189.
13. De Castro L.N., Von Zuben F.J. Learning and optimization using the clonal selection principle // IEEE Transactions on Evolutionary Computation. – Vol. 6. – № 3. – 2002. – pp. 239-251.
14. Васильев В. И. Интеллектуальные системы защиты информации: учеб. пособие / В. И. Васильев. 3-е изд., испр., и доп. – М.: Инновационное машиностроение, 2017. – 201 с.
15. KDD Cup 1999 Data [Electronic resource]. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 05.02.2018).

16. Zaind A., Maarof M., Shamsnddin S., Abraham A. Ensamble of One-class Classifier for Network Intrusion Detections. [Electronic resource]. URL: http://www.softcomputing.net/ias08_1.pdf (accessed 29.02.2018).
17. Mukkamala S., Sung A.H. Identifying Significant Features for Network Forensic Analysis using Artificial Intelligent Techniques // International Journal of Digital Evidence. – Vol. 1. – Issue 4. – 2003. – P. 1-17.
18. Mukkamala S., Sung A.H., Abraham A. Modeling Intrusion Detection Systems Using Linear Genetic Programming Approach. [Electronic resource]. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.544&rep=rep1&type=pdf (accessed 29.02.2018).
19. Chou T.S., Yen K.K., LNO J. Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms // International Journal Of Computational Intelligence. – Vol. 4. – № 3. – 2008. – pp. 196-208.
20. Мещеряков Р. В., Ходашинский И. А., Гусакова Е. Н. Оценка информативного признакового пространства для системы обнаружения вторжений // Известия ЮФУ. Технические науки. – № 12 (149). – Таганрог, 2013. – С. 57-63.
21. Виткова Л. А. Исследование распределенной компьютерной системы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. – №5. – 2015. – С. 44-48.
22. Ушаков С. А. Разработка и исследование алгоритмов решения задач распознавания на основе искусственных иммунных систем: диссертация на соискание ученой степени канд. техн. наук. – Воронеж, 2015. – 139 с.
23. Распределенные системы обнаружения атак // System-Repair.net [Электронный ресурс]. URL: http://systemrepair.net/2012/05/raspredelennye-sistemy-obnaruzheniya-atak/ (дата обращения: 31.03.2018).

V.V. Vasilyev, R.R. Shamsutdinov

INTELLIGENT NETWORK INTRUSION DETECTION SYSTEM BASED ON ARTIFICIAL IMMUNE SYSTEM MECHANISMS

Ufa State Aviation Technical University
Ufa, Russia

The article is devoted to the problem of detecting network attacks, both known and previously unknown. The application of various methods of artificial intelligence in the scientific literature to solve this problem was analyzed. The advantages of the artificial immune

system were revealed. Its main mechanisms including artificial lymphocytes generation, negative selection, clonal selection, data analysis, and periodic renewal of lymphocytes were analyzed. The article describes the developed intrusion detection system based on artificial immune system. Developed system includes a sniffing subsystem, so that allows it to analyze real data of host network connections. The article also describes network connections dataset KDD99, which used to efficiency evaluation of developed system. The methods of compressing the initial dataset proposed in the scientific literature were analyzed, and the drawbacks of these methods were identified. This article describes the experimental determination of the network connections significant parameters contained in the dataset. The authors identified 13 significant parameters from 41, and also they described the process of preliminary processing and preparation of the analyzed data, a series of experiments. The results of the experiments showed the high efficiency of the developed system in detecting unknown network attacks, detecting and classifying known attacks.

Keywords: intrusion detection system, artificial immune system, KDD99, information security, network security, network attack.

REFERENCES

1. Vasilyev V. I., Shamsutdinov R. R. Distributed Intrusion Detection System Based on Immune System Mechanisms, Information Technologies for Intelligent Decision Making Support, vol. 1, Ufa, 28-31 may 2018, pp. 237-244. (in Russian).
2. Kornev P. A., Pylkin A. N., Sviridov A. U. Using artificial intelligence in intrusion detection systems, Modern Problems of Science and Education, 2014, no. 6, pp. 135-143. (in Russian).
3. Branitsky A. A., Kotenko A. V. Analysis and Classification of Methods for Network Attack Detection, SPIIRAS Proceedings, St. Peterburg, 2016, no 2, pp. 207-244. (in Russian).
4. Zhigulin P.V., Podvorchan D. E. Analysis of network traffic on the basis of neural networks, Elektronnye sredstva i sistemy upravleniya [Electronic Tools and Control Systems], 2013, no. 2, pp. 44-48. (in Russian).
5. Shanmugavadivu R., Nagarajan N. Network intrusion detection system using fuzzy logic, Indian Journal of Computer Science and Engineering, available at: http://www.ijcse.com/docs/IJCSE11-02-01-034.pdf (accessed 29.03.2018).
6. Slepovichev I.I., Irmatov P.V., Komarova M.S., Bezhin A.A. DDos attack detection using fuzzy neural network, Izvestiya Saratovskogo universiteta. Seriya Matematika. Mekhanika. Informatika [News of Saratov University. Series: Mathematics. Mechanics. Informatics], 2009, no. 9, pp. 84-89. (In Russian).

7. Goyal A., Kumar C. GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System. Northwestern University, available at: http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf (accessed 29.03.2018).
8. Al-Enezi J.R., Abbod M.F., Alsharhan S. Artificial immune systems – models, algorithms and applications, Indian Journal of Computer Science and Engineering, 2010, vol. 2, no 3. pp. 118-131.
9. Bachmayer S. Artificial Immune Systems, Tietojenkäsittelytieteen laitos [Computer Science], available at: https://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/bachmayer.pdf (accessed 01.03.2018).
10. Tarakanov A.O., Tarakanov Y.A. A comparison of immune and genetic algorithms for two real-life tasks of pattern recognition, Int. J. of Unconventional Computing, 2004, vol. 1.4, pp. 357-374.
11. Tarakanov A.O., Tarakanov Y.A. A comparison of immune and neural computing for two real-life tasks of pattern recognition, International Conference on Artificial Immune Systems, Catania, 2004, pp. 236-249.
12. Vasilyev V.I., Kotov V.D. Network Attacks Detection System Based on the Mechanisms of Immune Model, Izvestiya YUFU. Tekhnicheskie nauki [News of SFedU. Technical Science], Taganrog, 2011, no. 12, pp. 180-189. (in Russian).
13. De Castro L.N., Von Zuben F.J. Learning and optimization using the clonal selection principle, IEEE Transactions on Evolutionary Computation. 2002, vol. 6, no. 3, pp. 239-251.
14. Vasilyev V. I. Intellektual'nye sistemy zashchity informacii [Intelligent information security systems], in Vasilyev V.I. (ed.), Innovacionnoe mashinostroenie Publ., Moscow, 2017, 201 p. (in Russian).
15. KDD Cup 1999 Data, available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 05.02.2018).
16. Zaind A., Maarof M., Shamsnddin S., Abraham A. Ensamble of One-class Classifier for Network Intrusion Detections, available at: http://www.softcomputing.net/ias08_1.pdf (accessed: 29.02.2018).
17. Mukkamala S., Sung A.H. Identifying Significant Features for Network Forensic Analysis using Artificial Intelligent Techniques, International Journal of Digital Evidence, 2003, vol. 1, no 4, pp. 1-17.
18. Mukkamala S., Sung A.H., Abraham A. Modeling Intrusion Detection Systems Using Linear Genetic Programming Approach, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.544&rep=rep1&type=pdf (accessed: 29.02.2018).

19. Chou T.S., Yen K.K., LNO J. Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms, International Journal Of Computational Intelligence, 2008, vol. 4, no. 3, pp. 196-208.
20. Meshcheryakov R.V., Khodashinsky I.A., Gusakova E.N. Evaluation of feature space for intrusion detection system // Izvestiya YUFU. Tekhnicheskie nauki [News of SFedU. Technical Science], Taganrog, 2013, no. 12, pp. 57-63. (in Russian).
21. Vitkova L.A. Study on distributed computer systems adaptive actions, H&ES Research, 2015, vol. 7, no. 5, pp. 44-48. (in Russian).
22. Ushakov S. A. Development and research of algorithms for solving recognition problems based on artificial immune systems, Abstract of Ph.D. dissertation, Theoretical foundations of computer science, Voronezh State University, Voronezh, Russian Federation, 2015. (in Russian).
23. Distributed attack detection systems, System-Repair, available at: http://systemrepair.net/2012/05/raspredelennye-sistemy-obnaruzheniya-atak/ (accessed 31.03.2018). (in Russian).