Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: bya@tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 88634371905.
Кафедра безопасности информационных технологий; доцент.

Bryukhomitsky Yuriy Anatoly
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: bya@tsure.ru.
2, Chekhov Street, Taganrog, 347928, Russia.
Phone: +78634371905.
The Department of Security in Data Processing Technologies; Associate Professor.

УДК 681.324

В.Д. Котов, В.И. Васильев

СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ НА ОСНОВЕ МЕХАНИЗМОВ ИММУННОЙ МОДЕЛИ

Системы обнаружения аномалий обладают большим потенциалом в области сетевой безопасности, однако на практике подобных систем реализовано мало. Хотя они способны обнаруживать атаки нулевого дня с приемлемым уровнем ложных срабатываний, существует проблема, связанная с необходимостью генерировать большое количество трафика, содержащего атаки. Подобные данные тяжело и дорого производить. В данной статье представлен адаптивный подход, основанный на иммунных механизмах. Поведение предлагаемой искусственной иммунной системы заимствует стратегию защиты у иммунной системы человека. В статье представлены результаты экспериментов, демонстрирующих перспективность технологии искусственных иммунных систем.

Система обнаружения вторжений; искусственные иммунные системы; адаптивные системы.

V.D. Kotov, V.I. Vasilyev

NETWORK ATTACKS DETECTION SYSTEM BASED ON THE MECHANISMS OF IMMUNE MODEL

The anomaly detection systems have big potential in the network security, but still too few of them are realized in practice. Although such systems can detect 0-day attacks with acceptable false alarm rate, the problem is that they have to be trained with the data, containing labeled attacks. And such data is hard and expensive to produce. This paper offers an adaptive solution based on the immunity mechanisms. The behavior of artificial immune system we proposed deploys the defense strategy of the human immunity. We show experimental results which demonstrate the efficiency of the artificial immune system technology.

Intrusion detection system; artificial immune systems; adaptive systems.

Введение. Система обнаружения вторжений (СОВ) является важным компонентом защиты компьютерных сетей. Её основная задача – это мониторинг сети или системы на предмет вредоносной активности. Несмотря на то, что проблема детектирования сетевых атак является довольно старой, она до сих пор актуальна. Не-

сколько лет назад вторжения в сеть были редким явлением, поскольку для их осуществления требовались обширные знания операционных систем, сетевых протоколов и т.п. Сегодня же любой пользователь способен осуществлять вредоносные действия в сети, загрузив одну из программ-эксплойтов, доступных в Интернете.

Одним из наиболее популярных направлений разработки систем компьютерной безопасности сегодня является технология искусственных иммунных систем [1]. Предполагается, что использование методов и техник защиты организма от микробов и вирусов позволит преодолеть проблемы классических средств обеспечения защиты информации.

В данной работе предпринимается попытка создания системы обнаружения вторжений, основанной на иммунной модели. За основу взята архитектура СОВ, разработанная Кимом и Бентли, которая называется иммунной моделью обнаружения вторжений [2]. Среди прочих она наиболее точно имитирует поведение биологической иммунной системы. Однако, по мнению авторов настоящей статьи, некоторые свойства иммунитета отсутствуют в модели Кима и Бентли, что отрицательно сказывается на её эффективности.

В статье рассмотрены механизмы иммунной системы и вычислительных алгоритмов на её основе, дано описание предлагаемого подхода. В конце статьи приведены результаты экспериментов.

1. Таксономия систем обнаружения вторжений. Система обнаружения вторжений – это устройство или программа, предназначенная для мониторинга активности системы или сети на предмет нарушений политики безопасности. Общая классификация современных подходов к детектированию сетевых атак может быть представлена следующим образом:

1. По типу объекта мониторинга:
   a) *хостовые СОВ* – осуществляют мониторинг активности одного узла в сети;
   b) *сетевые СОВ* – объектом мониторинга является сетевой сегмент.
2. По архитектуре:
   a) *централизованные* – все вычисления совершаются на одной рабочей станции;
   b) *распределенные* – система состоит из нескольких элементов: сенсоров, разнесенных по сети, вычислительного центра, а также консоли администратора.
3. По технологии анализа:
   a) *без сохранения состояния* – каждое событие рассматривается независимо от других;
   b) *с сохранением состояния* – информация о предыдущих событиях сохраняется и учитывается при принятии решения.
4. По методу обнаружения атак:
   a) *системы обнаружения злоупотреблений* – осуществляют поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных;
   b) *системы обнаружения аномалий* – обладают профилем нормальной активности системы и детектируют отклонения от него.

Согласно представленной классификации, предлагаемый в данной работе подход относится к распределенным сетевым системам обнаружения аномалий.

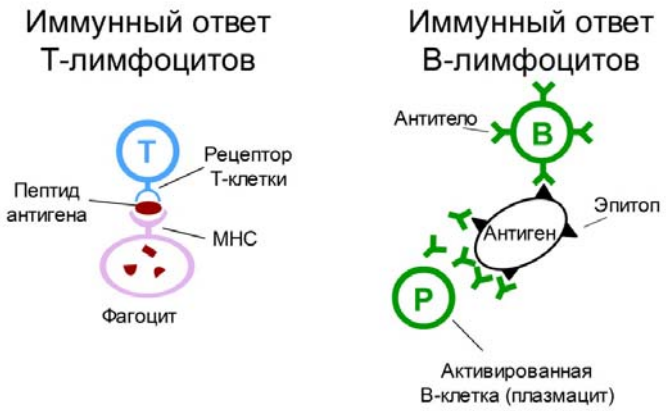
2. Обзор иммунной системы. Иммунная система представляет собой распределенный многоуровневый механизм защиты от чужеродных микроорганизмов, вирусов и патогенов. Каждый уровень иммунитета осуществляет свой тип защитной реакции, причем, чем выше уровень, тем выше специфичность ответа.

С точки зрения информатики, наиболее интересным является приобретенный иммунитет, поскольку обладает свойствами адаптивности и иммунной памяти. Основным участниками адаптивного иммунного ответа являются лимфоциты. Они бывают двух видов – Т и В.

Т-лимфоциты (или Т-клетки) способны распознавать патогенны, презентованные на поверхности других клеток (например, фагоцитов) с помощью рецепторов Т-клетки (рис. 1,а). Однако перед тем как Т-лимфоциты попадают в кровеносную систему для выполнения этой задачи, они проходят отрицательный отбор. Этот механизм позволяет отсеять те Т-клетки, которые способны реагировать на собственные антигены организма. Такие лимфоциты не нужны в иммунной системе, поскольку могут вызвать своего рода «ложные срабатывания».

В-клетки реагируют на заражение иным образом. Каждый В-лимфоцит несет на своей поверхности набор рецепторов – антител (рис. 1,б). Эти рецепторы способны распознавать особые молекулярные структуры антигенов – эпитопы. Будучи активированной, В-лимфоцит выделяет антитела, которые покрывают антиген. В таком состоянии его уничтожают другие клетки иммунитета, в частности фагоциты.

В-клетки осуществляют адаптивный иммунный ответ с помощью механизма клональной селекции. Активированная В-клетка размножается, причем каждая копия претерпевает мутацию. В итоге лимфоциты, которые в результате мутации получили способность лучше связываться с антигенами, становятся клетками памяти и сохраняются в организме на длительное время. Поэтому в следующий раз одному и тому же вирусу будет дан более эффективный иммунный ответ.



а б

Рис. 1. Распознавание чужеродного элемента В- и Т-лимфоцитами

В иммунологии существует также теория иммунных сетей, согласно которой лимфоциты могут быть активированы в отсутствие антигена. Причина такого поведения – это способность антител узнавать друг друга, образуя химическую связь. В результате образуется сеть связанных антител. Такое поведение клеток позволяет поддерживать в организме определенный репертуар агентов иммунитета. При появлении в иммунной сети чужеродного элемента активируется ответная реакция.

3. Классификация на основе иммунокомпьютинга. Иммунокомпьютинг [3] – это концепция машинного обучения, основанная на модели формального протеина и иммунной сети. Одним из исходных положений данной технологии является тот факт, что взаимодействие протеинов в иммунной сети может быть описано с помощью механизма сингулярного разложения ортогональных матриц.

Ключевой моделью иммунокомпьютинга является формальная иммунная сеть. Иммунная сеть W представляет собой множество клеток V_i, $W=\{V_1 \ldots V_m\}$. Клетка V представляет собой дуплет V=(c, P), где $c \in \mathbb{N}$ – класс клетки, $P = (p_1 \ldots p_q) \in \mathbb{R}^q$ – вектор в q-мерном Евклидовом пространстве, лежащий внутри единичного гиперкуба ($\|P\| \leq 1$). Метрика $d(V_i, V_j)$ представляет собой расстояние между двумя клетками, такое, что $d(V_i,V_j)= \|P_i - P_j\|$, где $\|P\|$ означает одну из возможных метрик (например, Евклидова норма или норма Чебышева и т.п.).

Клетка V_i «узнает» клетку V_j, если обе клетки относятся к одному и тому же классу и расстояние между ними меньше порогового значения h, $d(V_i, V_j) \leq h$.

Существует два правила поведения формальной иммунной сети W:

- Апоптоз – если клетка V_i «узнает» клетку V_j, то удалить V_i из W.
- Иммунизация – если V_i является ближе к V_j чем все остальные клетки иммунной сети W, то добавить V_i в множество W.

Процедура классификации на основе иммунокомпьютинга сводится к проецированию входного образа в пространство формальной иммунной сети и присвоение ему класса ближайшей клетки ФИС. Пусть $A=[a_1,a_2,\ldots,a_N]^T$ – матрица, строки которой представляют собой набор обучающих векторов свойств, т.е. a_i – это один обучающий образ. Путем сингулярного разложения мы можем представить матрицу A в виде произведения A=USV, где U и V это матрицы правых и левых сингулярных векторов, а S – диагональная матрица сингулярных чисел. Тогда проекция входного образа Z в пространство ФИС может быть вычислена по формуле

$$w_i = \frac{1}{s_i} Z^T v_i, \tag{1}$$

где w_i – i-я величина энергии связи, s_i – i-е сингулярное значение матрицы A, v_i – i-й правый сингулярный вектор матрицы A. Пространство ФИС бывает, как правило, одного, двух или трех измерений (i=1,2 или 3). Матрица U левых сингулярных векторов матрицы A представляет собой клетки формальной иммунной сети, к которым применяются вышеописанные правила.

Важным параметром иммунной сети является минимальное расстояние, на котором клетки узнают друг друга – h. Выбор наиболее подходящего порога активации происходит опытным путем, для этого формируется ФИС, после чего вычисляется его индекс нераздельности:

$$i = \ln(m_2) - \ln(m_1) - \ln(h). \tag{2}$$

Параметр m_1 в формуле (2) соответствует начальному числу клеток ФИС, m_2 – числу клеток после апоптоза и иммунизации, а h – порог узнавания клеток. Чем меньше индекс нераздельности, тем лучше качество распознавания иммунной сетью.

Алгоритм классификации на основе иммунокомпьютинга может быть представлен следующим образом:

Этап обучения:

1. Формирование обучающей матрицы.
2. Вычисление сингулярного разложения.
3. Апоптоз.
4. Иммунизация.
5. Вычисление индекса нераздельности.
6. Повторение шагов 3-5 с другими значениями h.
7. Выбор ФИС с наименьшим значением индекса нераздельности.

Этап классификации:

1. Отображение входного образа в пространство ФИС.
2. Определение ближайшей клетки ФИС.
3. Назначение класса ближайшей клетки входному образу.

В предлагаемом подходе используется вышеописанная процедура классификации на основе иммунокомпьютинга, однако в отличие от оригинального варианта, обучающая выборка частично генерируется автоматически с помощью алгоритма отрицательного отбора.

4. Алгоритм отрицательного отбора. В основе алгоритма отрицательного отбора [4] лежит механизм созревания Т-лимфоцитов в тимусе. Входными данными для алгоритма служит набор строк, состоящих из символов определенного алфавита (это могут быть числа, буквы и т.д.). Рассмотрим в качестве примера следующий набор строк S:

0010, 1000, 1001, 0000, 0100, 0010, 1001, 0011.

Целью алгоритма является сгенерировать набор детекторов – строк, каждая из которых не совпадает ни с одной строкой из S. Сначала необходимо сгенерировать набор случайных строк R_0:

0111, 1000, 0101, 1001.

Из этого набора необходимо выбрать те строки, которые не совпадают ни с одной строкой из S. Такими строками являются 0111 и 0101.

Если в последней строке набора S изменится один бит (она станет 0111), то детектор сможет зафиксировать это изменение.

Алгоритм отрицательного отбора состоит их двух этапов:

1) создание детекторов, при котором генерируется необходимое число детекторов на основе нормальных данных;
2) мониторинг системы, иными словами, сопоставление вновь поступившей порции данных с каждым из детекторов.

Следует отметить, что для успешной работы алгоритма не обязательно полное совпадение двух строк. Так, например, если рассматривать входные данные не как строки, а как вектора, состоящие из целых или вещественных чисел, то можно использовать одну из норм, таких как норма Чебышева, Евклида. В предлагаемом подходе степень сходства между векторами определяется расстоянием Хэмминга.

5. Алгоритм клональной селекции. Алгоритм клональной селекции [5] относится к классу эволюционных алгоритмов и применяется для решения задач оптимизации. Ключевым понятием данного алгоритма является аффинность. В иммунологии – это степень совместимости двух клеток, с точки зрения математической реализации – это значение оптимизируемой функции. В ходе алгоритма генерируется популяция антител *P* – набор случайно сгенерированных аргументов оптимизируемой функции. После этого вычисляется аффинность каждого антитела. Затем каждое антитело «клонируется», т.е. создается несколько копий антитела, причем, чем лучше аффинность антитела, тем больше клонов будет создано. Далее каждое антитело (включая клоны) претерпевает мутацию и, чем лучше аффинность данного антитела, тем меньше производится мутаций. Под мутацией понимается внесение случайных изменений в элементы антитела.

После мутации снова вычисляется аффинность каждого антитела. В результате выбирается *n* антител с лучшей аффинностью. Эти антитела заносятся в фонд клеток памяти *M*. После чего *n* худших антител начальной популяции *P* заменяется антителами из *M*.

В предлагаемом подходе алгоритм клональной селекции применяется для повышения качества детектирования атак и снижения уровня ложных срабатываний.

6. Предлагаемый подход.

6.1. Архитектура подхода. Как показано на рис. 2, архитектура предлагаемой системы состоит из следующих элементов:

1. Тимус – модуль ответственный за создание и селекцию детекторов. Тимус периодически генерирует новую порцию детекторов, постоянно обновляя их пул. Каждому детектору соответствует значение пригодности, которое в первом поколении равно нулю.
2. Классификатор – модуль, отвечающий за назначение классов вновь поступившим данным. Классификатор основан на формальной иммунной сети. Обучение ФИС происходит на нормальном трафике и детекторах. Когда появляется новая популяция детекторов, процедуры апоптоза и иммунизации повторяются.
3. Блок ответной реакции – представляет собой систему обратной связи, с помощью которой администратор безопасности может оценивать насколько корректно была обнаружена атака. В результате меняются значения пригодности детекторов.

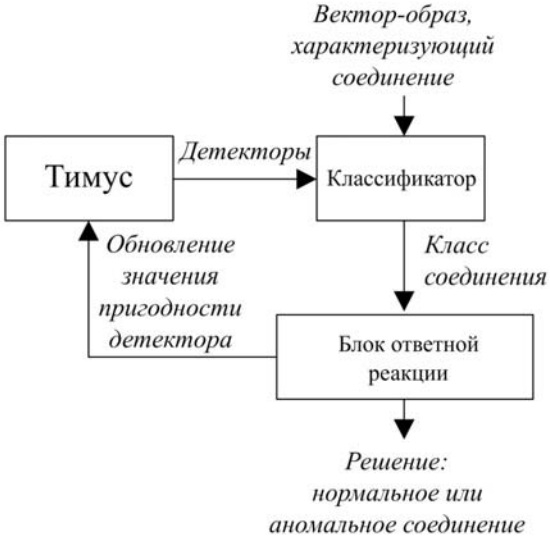


Рис. 2. Архитектура предлагаемого подхода

Данная модель имитирует поведение лимфоцитов в организме. По сути, детекторы постоянно генерируются и «циркулируют» в сети. Это позволяет поддерживать высокий уровень обнаружения, но при этом не генерировать слишком много данных.

6.2. Выбор параметров. Системы обнаружения аномалий, как правило, оперируют векторами свойств, характеризующих событие, связанное с безопасностью. Наша система предназначена для анализа сетевого трафика. Событие здесь соответствует одному соединению, если это протокол TCP и одному сетевому пакету, если это UDP или ICMP (пакеты рассматриваются как соединения с длительностью равной нулю). Сетевое соединение представляется в виде набора параметров, характеризующих его. В [6] авторы предложили 41 параметр, характеризующий соединение с трех сторон:

1. Внутренние параметры – данные полученные из заголовков пакетов, такие как число указателей срочности или флаги TCP.
2. Параметры содержимого – сюда входят такие показатели как количество полученных сеансов суперпользователя, попыток авторизации, создания файлов и т.п.
3. Параметры трафика – к этой категории относятся параметры, полученные с помощью скользящего окна в две секунды, это, например, число соединений к одному узлу или порту.

Данные параметры были использованы в предложенном подходе. Однако вторая группа параметров требует знания устройства сети, наличие профилей приложений, запускаемых на рабочих станциях. Использование второй группы свойств снижает универсальность подхода, поэтому в нашей системе использованы только первая и третья группы.

Следует также отметить, что предлагаемая СОВ осуществляет мониторинг отдельно по каждому протоколу прикладного уровня. Так, например, для контроля HTTP трафика используются только данные касающиеся веб-сервера, а для контроля SMTP – только данные почтовых серверов и т.д.

6.3. Представление данных. Поскольку мы используем параметры первой и третьей группы, описанные в предыдущем разделе, то вектор, характеризующий соединение, состоит из 25 элементов. Большинство параметров представляет собой вещественные числа, что лишает нас возможности генерировать детекторы на основе таких векторов (поскольку число детекторов получилось бы бесконечно большим). Для решения этой проблемы необходимо ввести конечный алфавит, из которого состояли бы вектора-образы.

Для дискретизации параметров используется нечеткая логика. Каждый параметр может быть отнесен к одному из нижеперечисленных нечетких множеств:

1. Меньше чем минимальное значение – такую характеристику параметр получит в случае, если его значение выходит за пределы его минимальной величины в обучающих данных.
2. В окрестности минимального значения – значение параметра находится в окрестности точки на числовой оси, равной минимальному значению параметра в обучающей выборке.
3. Среднее значение – значение параметра находится в окрестности точки на числовой оси, равной среднему арифметическому всех значений данного параметра в обучающей выборке.
4. В окрестности максимального значения – то же, что п. 2, но касательно максимального значения параметра в обучающей выборке.
5. Больше чем минимальное значение – то же, что п. 1, но касательно значения параметра в обучающей выборке.

Каждый параметр $s_i \in [s_i^{min}; s_i^{max}]$, представлен как значение функции принадлежности к нечетким множествам, описываемым вышеперечисленными лингвистическими переменными (рис. 3).

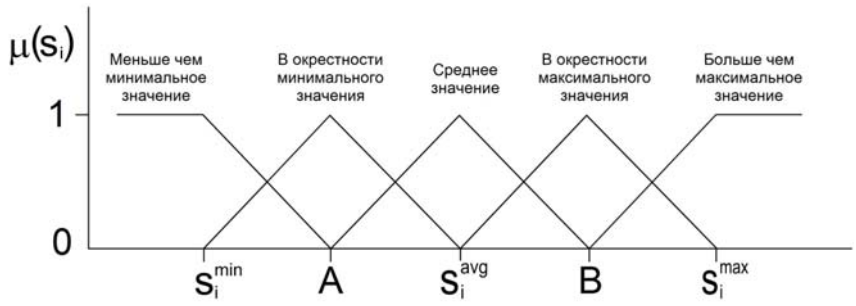


Рис. 3. Функции принадлежности нечетких множеств

Среднее значение каждого параметра $s_i^{avg} = \frac{s_i^{max} - s_i^{min}}{2}$, а также функция принадлежности генерируются в процессе обучения, при этом A и B равны $s_i^{avg} - 50\,\%$ и $s_i^{avg} + 50\,\%$ соответственно.

Для дефаззификации использовались следующие правила:

- ЕСЛИ s_i меньше чем минимальное значение, ТОГДА $s_i' = 0$.
- ЕСЛИ s_i в окрестности минимального значения, ТОГДА $s_i' = 1$.
- ЕСЛИ s_i среднее значение, ТОГДА $s_i' = 2$.
- ЕСЛИ s_i в окрестности максимального значения, ТОГДА $s_i' = 3$.
- ЕСЛИ s_i больше чем минимальное значение, ТОГДА $s_i' = 4$.

Дефаззифицированные значения s_i' параметров будут составлять вектора образы в предлагаемом подходе.

6.4. Создание детекторов и классификация. Детекторы генерируются с помощью алгоритма отрицательного отбора. В предлагаемом подходе каждый детектор это вектор из 25 элементов. Элемент вектора выбирается случайным образом из множества $Q = \{0, 1, 2, 3, 4\}$. В качестве меры расстояния между двумя векторами будет применяться расстояние по Хэммингу.

Детекторы, сгенерированные с помощью алгоритма отрицательного отбора, а также нормальный трафик подаются на вход классификатора на основе ФИС. Для обучения иммунной сети создается матрица $A = \binom{F}{R}$, где F – матрица, образованная нормальными векторами образами, R – матрица образованная детекторами. Следующим шагом вычисляется сингулярное разложение матрицы A. В результате образуются матрица U, состоящая из правых сингулярных векторов, матрица V левых сингулярных векторов и диагональная матрица S сингулярных чисел. Клетки иммунной сети представлены матрицей

$$U' = \begin{pmatrix} u_{11} & \cdots & u_{13} \\ \vdots & \ddots & \vdots \\ u_{N1} & \cdots & u_{N3} \end{pmatrix},$$

где N – число входных образов (а также число строк в матрице A). Каждому вектору соответствует один из двух классов: нормальный трафик или аномальный трафик. Далее идет процедура обучения, описанная в разд. 3.

Каждый вновь поступивший вектор-образ проецируется в трехмерное пространство ФИС с помощью формулы (1), после чего ему назначается класс ближайшей клетки иммунной сети. Если возникла аномалия, администратору предоставляется информация о происшествии и на её основе он должен оценить, корректна ли была классификация. При корректной классификации, уровень пригодности детектора, соответствующего среагировавшей клетке ФИС, увеличивается, в противном случае он уменьшается либо остается прежним, если решение о правильности назначенного класса невозможно принять.

Периодически искусственная иммунная система обновляется. По сути, к детекторам применяется алгоритм клональной селекции. Детекторы с большим значением пригодности претерпевают малые мутации или не мутируют вообще, в то время как мало пригодные детекторы меняются в значительной степени. В отличие от оригинального алгоритма клональной селекции, в предлагаемом подходе число клонов ограничено десятью, при этом 20 % детекторов, обладающих наименьшими значениями пригодности, заменяются новой популяцией.

7. Эксперименты. Подход был проверен на наборе трафика DARPA Intrusion Detection Data Set [7], полученном в ходе работы симуляционной модели вычислительной сети ВВС США.

Для оценки эффективности предложенной системы использовалось два параметра:

1) уровень обнаружения аномалий

$$TP = \frac{N_{TP}}{N_{TP} + N_{FN}},$$

где N_{TP} – число корректных обнаружений, N_{FN} – число пропусков атак;

2) уровень ложных срабатываний

$$FP = \frac{N_{FP}}{N_{FP} + N_{TN}},$$

где N_{FP} – число ложных срабатываний, N_{TN} – число корректно классифицированных нормальных векторов.

На рис. 4 данные параметры показаны в динамике за 10 шагов.

Поскольку нам заранее известно, какие векторы относятся к атакам, в данном эксперименте работа администратора по принятию решений о корректности классификации была автоматизирована.

Таблица 1

Результаты эксперимента

Число шагов	Уровень обнаружения	Уровень ложных срабатываний
500	0,83	0,12
1000	0,83	0,11
5000	0,85	0,11

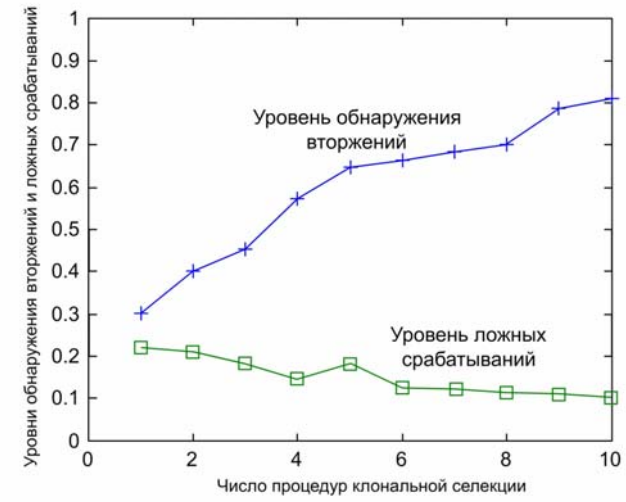


Рис. 4. Показатели эффективности подхода за десять шагов

Как видно из таблицы, уровни обнаружения и ложных срабатываний стабилизируются после большого числа шагов. В ходе эксперимента была выявлена проблема, которая заключается в том, что некоторые вектора постоянно мигрируют из области нормального трафика в область аномального трафика. Из-за процедуры дискретизации параметров часть векторов, соответствующих атакам, стала идентична векторам из обучающей выборки (которая не содержит атак), что вносит дополнительный вклад в уровень ложных срабатываний.

Заключение. В ходе исследования рассмотрена задача реализации алгоритмов иммунной системы для обнаружения вторжений в сеть. Особенностью подхода является автоматическое создание обучающих данных, представляющих вредоносный трафик. Предложенный подход может быть использован в реальной вычислительной среде, поскольку нет необходимости генерировать трафик, содержащий атаки, который необходим в других подходах. Подобный трафик тяжело и дорого создавать, поэтому классические системы обнаружения аномалий трудно применять в реальных условиях.

В перспективе вычислительная техника должна поддерживать десятки миллионов детекторов, именно таков порядок числа лимфоцитов в нашем организме. Мощности современных компьютеров пока не хватает для того, чтобы полностью имитировать иммунный ответ и покрыть всё пространство атак.

В связи с этим необходимо продолжать исследования в этой области и искать новые способы представления данных и создания искусственных антител.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Яремчук С.* Иммунная система для компьютера // Системный администратор. – 2004. – № 11. – С. 48-51.
2. *Kim J., Bentley P.* An Artificial Immune Model for Network Intrusion Detection. Интернет ресурс, режим доступа: http://*neuro.bstu.by/our/immune3.pdf*, дата доступа: 5 октября 2011 г.
3. *Tarakanov A.O.* Immunocomputing for Intelligent Intrusion Detection. IEEE Computational Intelligence Magazine. – 2008. – С. 23-30.
4. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonself discrimination in a computer, Proc. of 1994 IEEE Symposium on Research in Security and Privacy, 1994. – С. 202-212.
5. *De Castro L., Fon Zuben F.* Learning And Optimisation Using Clonal Selection Principle IEEE Transactions on Evolutionary Computation, Special Issue On Artificial Immune Systems, 2002. – № 6. – С. 239-251.
6. *Stolfo S.J., Fan W., Lee W., Prodromidis A., Chan Ph. K.* Cost-based Modeling and Evaluation for Data Mining With Application to Fraud and Intrusion Detection: Results from the JAM Project, Интернет ресурс, режим доступа*:* weifan.info/PAPERS/JAM99.pdf, дата доступа: 5 октября 2011 г.
7. MIT Lincoln Laboratory Cyber Systems & Technology: DARPA Intrusion Detection. Интернет ресурс, режим доступа: http://www.ll.mit.edu/mission/communications/ist/CST/, дата доступа: 5 октября 2011 г.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Котов Вадим Дмитриевич
Уфимский государственный авиационный университет.
E-mail: vadim_kotov@ieee.org.
450000, г. Уфа, пр. К. Маркса, 12.
Тел.: 83472730672.
Кафедра вычислительной техники и защиты информации; аспирант.

Васильев Владимир Иванович
E-mail: vasilyev@ugatu.ac.ru.
450092, г. Уфа, ул. Авроры, 3, кв. 40.
Кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

Kotov Vadim Dmitrievich
Ufa State Aviation Technical University.
E-mail: vadim_kotov@ieee.org.
12, Karl Marx Street, UFA, 450000, Russia.
Phone: 83472730672.
The Department of Computer Engineering and Information Security; Postgraduate student.

Vasilyev Vladimir Ivanovich
E-mail: vasilyev@ugatu.ac.ru.
3, Aurora Street, Apts, 40, Ufa, 450092, Russia.
The Department of Computer Engineering and Information Security; Dr. of Eng. Sc.; Professor.