УДК 004.056
doi:10.15217/issn1684-8853.2015.4.69

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК НА ОСНОВЕ КОМПЛЕКСИРОВАНИЯ НЕЙРОННЫХ, ИММУННЫХ И НЕЙРОНЕЧЕТКИХ КЛАССИФИКАТОРОВ

А. А. Браницкий[a], *младший научный сотрудник*
И. В. Котенко[a], *доктор техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Постановка проблемы: *несовершенство существующих методов обнаружения вторжений, а также изменяющийся характер вредоносных действий со стороны атакующего приводят компьютерные системы в небезопасное состояние, поэтому важно идентифицировать новые типы атак и своевременно реагировать на них.* ***Цель:*** *разработка гибридной схемы обнаружения и классификации сетевых атак на основе комбинирования адаптивных классификаторов.* ***Результаты:*** *предложена обобщенная схема комбинирования классификаторов для обнаружения сетевых атак. На ее основе разработано программное средство, которое позволяет анализировать сетевой трафик на наличие аномальной сетевой активности. Для уменьшения числа используемых признаков предлагается применять метод главных компонент. Основными особенностями предлагаемого подхода является многоуровневый анализ сетевого трафика, а также использование различных адаптивных модулей в процессе обнаружения атак. Проведены вычислительные эксперименты на двух открытых наборах данных с использованием различных способов комбинирования классификаторов.* ***Практическая значимость:*** *разработанные модули могут быть использованы для обработки данных, полученных от сенсоров системы управления информацией и событиями безопасности.*

Ключевые слова *— обнаружение вторжений, сетевые атаки, нейронные сети, иммунные детекторы, нейронечеткие классификаторы, метод главных компонент.*

Введение

Обнаружение сетевых атак является одной из актуальных проблем защиты информации вследствие быстрого развития компьютерных технологий и несовершенства существующих методов обнаружения атак. В целях исправления сложившейся в этой области ситуации текущие усилия исследователей направлены на поиск и применение новых, в том числе гибридных и адаптивных, схем обнаружения.

В данном исследовании предпринята попытка выявления сетевых атак на основе анализа соединений, характеризующих деятельность удаленных хостов. В этом случае мониторинг сетевой активности, как правило, состоит из следующих этапов. На первом этапе осуществляется фильтрация входящих и исходящих пакетов, собранных с помощью агентов-сенсоров, установленных в контролируемых узлах сети. На данном этапе также происходит агрегация пакетов для формирования признаков установленной сессии относительно уникальной пары сокетов. На следующем этапе собранные с первого уровня данные помещаются в хранилище для их последующей обработки и интерпретации. На последнем этапе происходит уведомление администратора об обнаруженных изменениях в политике безопасности и предлагаются возможные способы решения для предотвращения дальнейшего хода развития вторжения.

В настоящей работе задача обнаружения сетевых атак решается на основе применения гибридного подхода, особенностью которого является комплексирование использования традиционной модели обнаружения, основанной на сигнатурном подходе, и нескольких дополнительных моделей — статически обученных нейронных сетей, нейронечетких классификаторов и динамически обучающихся иммунных детекторов, что позволяет говорить о реализации многоуровневого и адаптивного обнаружения сетевых атак. Использование нейронных сетей и нейронечетких классификаторов предполагает, что характер действий нарушителя с течением времени остается постоянным и предсказуемым. При применении иммунных детекторов принимается во внимание динамическая составляющая поведения атакующего: в режиме обнаружения классификаторы продолжают обучаться на новых признаках обнаруженных атак. В целях ускорения обучения, тестирования и запуска детекторов применяется также алгоритм, реализующий метод главных компонент.

Релевантные работы

В настоящее время существует множество работ, в которых исследуется применимость рассматриваемых методов в задачах обнаружения атак. Представим некоторые из этих работ более детально. В качестве обучающего множества для искусственных нейронных сетей могут служить

различные данные. Так, в работах [1, 2] для решения поставленной задачи предлагается использовать многослойную нейронную сеть, обученную на данных из множества сигнатур Snort. Во многих работах, например [3–5], в качестве обучающих данных используется множество записей KDD Cup 99. Еще одним источником данных являются смоделированные соединения. Примером работы, в которой автор использовал трехслойную нейронную сеть прямого распространения в качестве бинарного классификатора сетевых соединений, является статья [6]. Данные работы объединяет общая идея применения одного классификатора, направленного на выявление нелегитимного трафика.

Другие авторы [7, 8] предлагают модель иммунной системы с жизненным циклом Т-лимфоцитов, в которой учитывался процесс их созревания в тимусе, а также активация, формирование клеток иммунной памяти через сигнал костимуляции и гибель иммунных клеток. Разработанная ими система LISYS (*Lightweight Immune SYStem*) предназначена для обнаружения вторжений в распределенной среде. Хотя эта система обладает рядом преимуществ, включая относительно небольшие вычислительные издержки, надежность и масштабируемость, авторы отмечают некоторые из недостатков. Среди них — невозможность обнаружения сетевых атак с применением протокола UDP и возможность обмануть систему путем проведения распределенных во времени атак типа медленного сканирования. Работа [9] предоставляет обзор двухуровневой системы обнаружения вторжений, в которой совмещены преимущества иммунных систем и сетей Кохонена. На первом этапе происходит фильтрация признаков сетевых соединений с помощью иммунных детекторов, обученных по методу отрицательного отбора, тем самым отсеиваются те образцы, которые соответствуют нормальным соединениям. На втором этапе аномальные экземпляры обрабатываются самоорганизующимися картами и группируются в отдельные кластеры со схожими признаками. В работе [10] также представлена двухуровневая модель, в которой для обнаружения аномалий использовались иммунные системы, а для обнаружения злоупотреблений — нейронные сети с методом главных компонент.

Применение нейронечетких систем к задачам обнаружения вторжений обсуждалось в работах [11–13]. Их авторы использовали параметры наборов данных KDD Cup 99 и DARPA 1998 как входные данные для нечетких классификаторов, построенных на основе нечеткого вывода Сугено.

Существуют также различные гибридные подходы, например комбинирование аппарата иммунных систем и нейронных сетей [14–16]. В качестве иммунных детекторов выбраны многослойные нейронные сети, которые генерируются при помощи метода клональной селекции. Эксперименты были проведены на наборе данных KDD Cup 99, они доказали высокую способность детекторов приспосабливаться к новым типам атак.

Другим гибридным решением задачи обнаружения вторжений является комбинирование нескольких нейронных сетей в единый классификатор. Так, работа [17] посвящена применению метода SVM и радиально-базисных сетей для классификации записей из набора данных NSL-KDD. Итоговый классификатор представляется как композиция последовательно построенных на разных выборках классификаторов и процедуры простого голосования. В результате уровень классификации удалось повысить примерно на 1,6 % по сравнению с классификаторами, взятыми по отдельности. Другие авторы [18, 19] предлагают подавать выходные значения от нескольких нейронных сетей, обученных различными алгоритмами, на вход процедуры взвешенного голосования и голосования по большинству. На тестовой выборке, состоящей из 6890 образцов, достигнута точность классификации выше 99 %.

Статья [20] описывает двухуровневую схему обнаружения и классификации атак. Несколько адаптивных нейронечетких модулей объединены вместе. Каждый из них предназначен для обнаружения только одного класса соединений и обрабатывает параметры записей KDD Cup 99. Итоговая классификация выполняется нечетким модулем принятия решений, который реализует систему нечеткого вывода Мамдани с двумя функциями принадлежности. Этот модуль ответственен за определение того, насколько аномальной является обрабатываемая запись. Ее класс соответствует классу нечеткого модуля первого уровня с наибольшим выходным значением.

В настоящей статье предложен подход, развивающий рассмотренные работы. Он основан на реализации многоуровневого и адаптивного обнаружения сетевых атак за счет комбинации нейронных сетей, иммунных систем и нейронечетких классификаторов. Адаптивные детекторы выполняют параллельную обработку входных признаков соединений. Детекторы обучены на различных выборках данных и предназначены для классификации одного соединения.

Классификаторы на основе нейронных сетей

При разработке общего подхода и программного средства для обнаружения и классификации сетевых атак была выбрана система из многослойных нейронных сетей с одним скрытым слоем. Каждая нейросеть состоит из трех слоев, в которых находятся идентичные по структуре вычислительные узлы, организованные таким образом, что выход одного нейрона соединяется

с входом каждого нейрона следующего слоя. Внешний слой нейронных элементов распределяет входные сигналы $\mathbf{X}^{(1)} = \left(\mathbf{x}_1^{(1)}, \ldots, \mathbf{x}_{29}^{(1)}\right)^{\mathrm{T}}$, представляющие собой вычисленные параметры сетевого соединения, на нейронные элементы скрытого слоя. Набор входных сигналов $\mathbf{X}^{(1)}$ представляет собой 29-мерный (по числу вычисляемых атрибутов сетевого трафика) вектор признаков рассматриваемого сетевого соединения. Каждый элемент этого вектора нормализован и представляет собой вещественное число в интервале [0;1]. Число нейронов в скрытом слое эвристически выбрано равным 20. Входной сигнал для каждого узла этого слоя представляет собой взвешенную сумму выходных сигналов всех узлов предыдущего слоя. Первый слой создает на входе активирующего элемента каждого узла второго слоя сигнал: $x_i^{(2)} = w_{i1}^{(1)} \cdot x_1^{(1)} + \ldots + w_{i29}^{(1)} \cdot x_{29}^{(1)} + \theta_i$, i = 1, ..., 20, $w_{ij}^{(1)}$ — веса, модифицирующие сигналы $\mathbf{X}^{(1)}$; θ_i — параметр смещения i-го нейрона скрытого слоя. Последний выходной слой состоит из одного нейронного элемента и осуществляет отображение преобразованных исходных сигналов в два класса, которые характеризуют тип атаки или нормальное соединение. Сигнал $X^{(3)}$, подаваемый на его вход, формируется следующим образом: $X^{(3)} = w_1^{(2)} \cdot \varphi\left(x_1^{(2)}\right) + \ldots + w_{20}^{(2)} \cdot \varphi\left(x_{20}^{(2)}\right) + \theta$, $\varphi(x)$ = th(x) — симметричная сигмоидальная функция активации; $w_j^{(2)}$ — весовые коэффициенты нейронов второго слоя; θ — параметр смещения выходного нейрона. Положительное значение выходного нейрона $\left(\varphi\left(X^{(3)}\right) > 0\right)$ характеризует атаку. Отрицательное значение на выходе $\left(\varphi\left(X^{(3)}\right) < 0\right)$ характеризует нормальное соединение. Для распознавания каждого типа атаки формируется отдельный нейросетевой детектор, выполняющий классификацию параллельно с остальными. Для его обучения используется обучающая выборка, состоящая из 50 % соединений одного из типов атак и 50 % нормального трафика. Для обучения нейросетевого классификатора применяется модифицированный алгоритм обратного распространения ошибки [21]. Среди его основных преимуществ можно отметить существенное увеличение скорости сходимости за счет динамической корректировки весов.

Классификаторы на основе иммунных систем

При построении иммунных детекторов в качестве основы была взята эволюционная модель с жизненным циклом, предложенная Хофмайером и Форестом (Hofmeyr and Forrest) [7] и дополненная реализацией двухступенчатой фазы обучения и способностью детекторов «делиться» между собой накопленными знаниями об угрозах.

Каждый иммунный детектор представляет собой самоорганизующуюся двухслойную сеть (карту) Кохонена. Первый слой распределяет входной сигнал $\mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_{29})^{\mathrm{T}}$ — вектор признаков сетевого соединения. Второй слой представляет собой двумерную квадратную решетку размером 15×15. Каждая компонента x_i $(1 \le i \le 29)$ входного сигнала связана с нейроном выходного слоя и имеет синаптический вес w_{ijk}.

В сетях Кохонена применяется конкурентное обучение. При подаче вектора на вход карты побеждает тот нейрон выходного слоя, вектор весов которого в наименьшей степени отличается от входного вектора. Для нейрона-победителя (i, j) выполняется соотношение $\mathrm{d}\left(\mathbf{X}, \mathbf{W}_{ij}\right) = \min\limits_{\substack{1 \le m \le 15 \\ 1 \le n \le 15}} \mathrm{d}\left(\mathbf{X}, \mathbf{W}_{mn}\right)$, где d($\mathbf{X}$, $\mathbf{W}_{ij}$) — расстояние между входным вектором $\mathbf{X}$ и весовым вектором нейрона-победителя $\mathbf{W}_{ij} = (\mathbf{w}_{1ij}, \ldots, \mathbf{w}_{29ij})^{\mathrm{T}}$.

В процессе обучения вокруг нейрона-победителя образуется окружение из тех нейронов, чьи веса близки к весовому вектору нейрона-победителя относительно выбранной метрики. Их веса корректируются по правилу Кохонена $\mathbf{W}_{pq}(t+1) = \mathbf{W}_{pq}(t) + \gamma\left(\mathbf{X} - \mathbf{W}_{pq}(t)\right)$, где γ — коэффициент скорости обучения; t — номер текущей итерации алгоритма; $1 \le p \le 15$, $1 \le q \le 15$.

Для распознавания каждого типа атаки выделяется несколько иммунных детекторов, которые обучаются на разных выборках из обучающего множества. За счет этого достигается создание уникальных классификаторов, разнообразных по своей структуре и способных реагировать на широкий спектр аномальной сетевой активности. После обучения детекторы подвергаются отрицательному отбору: для этого на их вход подается заранее подготовленная выборка, содержащая набор параметров только нормальных соединений. Те детекторы, которые распознали каждый элемент этого набора как нормальное соединение, допускаются к анализу сетевого трафика. Остальные классификаторы обучаются повторно по ранее настроенным весовым коэффициентам (рис. 1).

Первая группа иммунных детекторов, прошедших стадию отрицательного отбора, становится клетками памяти, наделяется бесконечным сроком жизни и допускается к анализу сетевого трафика без возможности обучения других иммунных детекторов (в случае обнаружения атаки они не добавляют параметры обнаруженного аномального соединения в обучающее

■ ***Рис. 1.*** Жизненный цикл иммунного детектора

множество). Другая группа классификаторов имеет конечный срок жизни. Если за отведенный период времени такой детектор не обнаружил ни одной атаки, он направляется на повторный этап обучения. В противном случае его срок жизни увеличивается, и он производит запись признаков нелегитимной сессии в обучающее множество. Поэтому новое поколение детекторов будет использовать расширенное обучающее множество данных и охватывать новый набор аномальных соединений. Тем самым описанная выше методика обучения иммунных детекторов включает в себя две стадии — настройку весовых коэффициентов с помощью образцов нелегитимного трафика и тестирование на предмет ложных срабатываний с помощью отрицательного отбора.

Стоит отметить, что существенное значение в корректности обнаружения вторжений при помощи иммунных детекторов имеет специально подобранное значение порога. Слишком малое его значение означает возможность пропуска атак, а слишком большое значение увеличивает число ложных срабатываний.

Нейронечеткие классификаторы

Данные классификаторы представляют собой пятислойную сеть прямого распространения сигнала, в которой реализован нечеткий вывод Такаги — Сугено. Входом для такой сети являются количественные значения сетевых параметров, выход сети — результат идентификации соединения. Для дискретизации каждого входного значения было выбрано пять лингвистических термов: {«малое», «небольшое», «среднее», «достаточно большое», «большое»}.

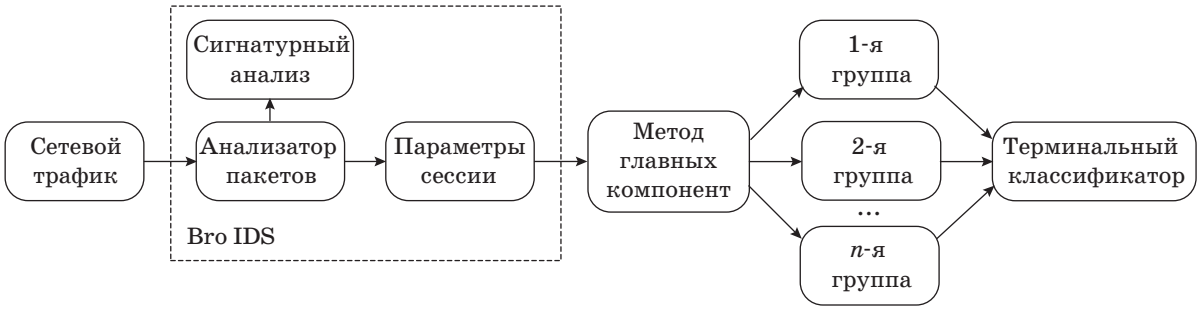
Первый слой вводит операцию фаззификации входных параметров и задает для них нечеткие термы. Для каждого терма этого слоя в качестве функции принадлежности выбрана колоколообразная функция $\left(1+\left|\frac{x-c}{a}\right|^{2b}\right)^{-1}$. Выходом этого слоя являются значения функций принадлежности для заданных значений входов. Второй слой задает антецеденты нечетких правил и осуществляет произведение входных сигналов или применяет операцию минимума для входных сигналов. Выход этого слоя — степень выполнения правил. Третий слой отвечает за нормализацию выходных значений предыдущего слоя. Каждый узел этого слоя вычисляет относительную степень выполнения входного нечеткого правила. В четвертом слое рассчитываются вклады каждого нечеткого правила в выход сети. Единственный узел пятого слоя агрегирует результат, полученный по каждому правилу. Для обучения применялся алгоритм обратного распространения ошибки и смешанный набор признаков соединений. Выход сети настраивался таким образом, чтобы он равнялся 1 в случае, если класс атаки соответствует типу данной сети, и –1 в противном случае.

Схема гибридизации

Предложенная обобщенная схема гибридизации сигнатурного и адаптивного подходов представлена на рис. 2.

Для анализа пакетов и формирования параметров сессии использовалась система Bro IDS [22], к которой были добавлены дополнительные скрипты для обработки сетевых событий. В системе имеется встроенный интерпретатор сценариев, который обеспечивает обработку различных сетевых событий.

При формировании записи о каждом сформированном соединении из поля данных и заголовка каждого пакета выделяются и вычисляются



■ ***Рис. 2.*** Схема гибридизации

параметры, необходимые для классификации соединений. Также собираются статистические сведения об открытых в данный момент соединениях. Опционально для уменьшения размерности входной вектор сжимается по методу главных компонент. Каждая группа детекторов, обученная для распознавания одного определенного типа соединения, обрабатывает последний набор признаков. Конечный результат классификации выдается терминальным классификатором.

В рамках этой схемы возможно применение нескольких методик обнаружения атак. Первая из них подразумевает, что каждая группа состоит из нескольких однотипных классификаторов, которые обучены на разных выборках из обучающего множества. Это позволяет создавать детекторы, которые отличаются друг от друга настроенными весовыми коэффициентами, и тем самым повышать количественные показатели обнаружения атак. Вторая методика предполагает применение гетерогенных классификаторов внутри каждой группы. Здесь для распознавания конкретного типа атаки использованы экземпляры каждой из трех моделей. В обоих случаях выходные значения от всех классификаторов могут быть рассмотрены как входной вектор для терминального классификатора.

Рассмотрим подробнее процесс обнаружения атак. Его можно разбить на три этапа.

На первом этапе осуществляется IP-дефрагментация сырых пакетов и сборка TCP-сегментов в сессии. Каждое соединение (сессия) есть последовательность TCP-пакетов за определенный временной интервал, в рамках которого происходит передача данных между парой удаленных хостов <addr_src, port_src> и <addr_dst, port_dst> с использованием определенного протокола. В процессе анализа сетевого трафика отслеживаются пакеты, инициирующие начало сессии (SYN) и служащие признаком ее завершения (FIN, RST, timeout). Каждую сессию можно охарактеризовать как набор параметров, элементы которого условно разбиты на две группы: атрибуты, полученные из заголовков пакетов (тип используемого протокола, признак равенства портов отправителя и получателя и т. п.), и статистические данные (количество соединений к заданному хосту в течение последних двух секунд, процентное число соединений к различным службам и т. п.). Кроме того, этот этап отвечает за первоначальное обнаружение сетевых аномалий путем проверки соответствия содержимого отдельных пакетов заданным регулярным выражениям в сигнатурном множестве.

Второй этап включает применение метода главных компонент и преобразование выходных параметров каждой сессии в сжатый набор атрибутов. Каждый элемент нового вектора есть линейная комбинация элементов старого вектора с коэффициентами, в роли которых выступают элементы собственных векторов матрицы ковариации исходных данных.

Третий этап представляет собой применение нескольких групп адаптивных классификаторов. Каждая группа состоит из детекторов, отвечающих за распознавание одного определенного типа соединения. Для повышения скорости классификации каждый детектор обрабатывает входящий набор параметров параллельно с остальными.

Терминальный классификатор может быть представлен несколькими способами. Простейший из них — процедура голосования по большинству. В этом случае классом соединения является тот, за который проголосовало большее количество детекторов внутри определенной группы. Другим методом для реализации терминального классификатора является взвешенное голосование [13] и его модификация — бустинг [23]. В этом случае каждому классификатору будет назначен соответствующий коэффициент, присвоенный ему в процессе обучения. Это позволит более обоснованно применять тот или иной классификатор в зависимости от его показателей корректности распознавания атак, вычисленных на образцах обучающего множества. Следующий подход заключается в выборе наилучшего классификатора для каждой конкретной записи и игнорировании остальных. Основной сложностью здесь является построение для каждого классификатора заданной области компетентности

в пространстве признаков [24]. Также предлагается использовать выходные значения от классификаторов первого уровня в качестве обучающего множества для терминального классификатора. Этот прием, известный как многоярусное обобщение (stacked generalization) [25], может быть построен на основе методов интеллектуального анализа данных.

Эксперименты

Для проверки описанных моделей были выбраны два открытых набора данных: KDD Cup 99 и NSL-KDD. Для этих наборов каждая запись представляет собой образ реальной сетевой сессии, описанной в виде набора из 41 параметра, и промаркирована как атака или нормальное соединение. Разработанная система обнаружения вторжений осуществляет мониторинг на уровне данных, полученных из пакетных заголовков, и статистических сведений, сформированных методом скользящего окна. Поэтому было выбрано 29 параметров, удовлетворяющих этому требованию. Кроме того, для классификации соединений выбрано 5 видов DoS-атак и 4 вида атак типа сканирование портов. Полученные от системы Bro данные обрабатываются модулями, в которых реализован механизм классификации соединений с применением предложенных детекторов. Для проверки эффективности функционирования моделей выбраны следующие численные показатели: $FP = \frac{n_{FP}}{n_{FP} + n_{TN}} \cdot 100\%$ — процентное количество образцов нормальных соединений, распознанных как атаки (false positive); $TP = \frac{n_{TP}}{n_{TP} + n_{FN}} \cdot 100\%$ — процентное количество верно распознанных образцов аномальных соединений (true positive); $CC = \frac{n_{CC}}{n} \cdot 100\%$ — процентное количество образцов сетевых соединений, класс которых был верно определен (correct classification). Значение порога для иммунных детекторов было выбрано экспериментальным путем таким образом, чтобы на обучающих данных выполнялось $TP - FP + CC \to \max$.

Результаты экспериментов для каждого подхода с указанными значениями этих параметров, в которых в качестве терминального классификатора использовалась процедура голосования по большинству, представлены в табл. 1.

Как видно из полученных результатов, нейросетевые и нейронечеткие классификаторы по сравнению с иммунными детекторами имеют большее число корректно распознанных соединений при анализе сетевых параметров. А значит эти классификаторы являются более предпочтительным инструментом при обнаружении сетевых атак. В то же время иммунные детекторы за счет динамической конфигурации весов способны модифицировать свою структуру в ответ на обнаруженные атаки. Поэтому в процессе анализа сетевого трафика показатели эффективности распознавания сетевых атак иммунными детекторами увеличиваются с течением времени. Этот механизм эволюции, а также обновляемый набор обучающих данных способствуют повышению распознавания ранее неизвестных типов атак.

Нейронные сети среди предложенных трех моделей показали наилучшую степень распознавания образцов сетевых соединений. Для нейронечетких классификаторов характерен длительный процесс обучения. Это объясняется трудоемкостью вычислений, связанной с многоуровневой структурой сети, и настройкой параметров функций принадлежности в нечетких правилах. Тем не менее показатель обнаружения атак для этих классификаторов является высоким и сопоставимым с показателем нейронных сетей.

Кроме того, для каждого типа атаки были вычислены показатели обнаружения различными детекторами. Так, в табл. 2 представлены показатели эффективности распознавания атак на наборе KDD Cup 99 комбинированными классификаторами. В представленной таблице левый столбец — тип соединения, верхняя строка — тип классификаторов, их пересечение — процентное число правильно распознанных атак.

Методом комбинирования отдельных классификаторов удалось добиться увеличения показателей обнаружения на 3,85 и 3,96 % по сравнению со средним значением этой величины для

■ ***Таблица 1***. Показатели *FP*, *TP*, *CC*

Подход	KDD Cup 99			NSL-KDD		
	FP	*TP*	*CC*	*FP*	*TP*	*CC*
Нейронные сети	3,56	98,95	73,56	7,08	98,24	56,86
Иммунные детекторы	2,26	91,16	94,82	12,51	93,06	65,65
Нейронечеткие классификаторы	11,65	98,29	88,89	16,94	96,37	83,06
Комбинация подходов	1,31	99,98	77,04	5,11	99,85	57,96

■ *Таблица 2*. Показатели эффективности распознавания атак комбинированными классификаторами, %

	back	neptune	pod	smurf	teardrop	ipsweep	nmap	ports-p	satan
back	100	0	0	0	0	0	0	0,46	3,37
neptune	0	99,98	0	0	0	0	0,56	99,99	99,93
pod	0	0	60,98	0	34,09	1,89	1,89	100	37,88
smurf	0	0	0	99,92	0	0	0,05	0	0,09
teardrop	0	0	56,63	0	100	0,2	0	100	100
ipsweep	0	0	0,4	0	0	100	91,95	1,69	0,4
nmap	0	0	0,43	0	0	44,16	100	44,59	44,59
ports-p	0,1	3,09	0,1	0	0	67,6	0,39	100	89,68
satan	0	88,64	0	0	0	9,28	0,25	88,26	99,87
normal	0,06	0,03	0,05	0,03	0	0,1	0,44	0,25	0,56

отдельных классификаторов соответственно для KDD Cup 99 и NSL-KDD. В то же время показатель корректной классификации остался выше этого показателя для нейронных сетей.

Построенная система обнаружения вторжений может быть использована в реальных компьютерных сетях после предварительного обучения на трафике, характерном для этой сети. В частности, в настоящее время исследование направлено на проведение экспериментов, связанных с новыми сгенерированными данными. С этой целью был создан программный стенд для моделирования компьютерной сети крупного предприятия, используемой для экспериментов с разработанной SIEM-системой [26] с учетом различных уязвимостей программно-аппаратного обеспечения [27].

Заключение

Представлена реализация гибридной системы обнаружения вторжений, предназначенной для анализа трафика в компьютерных сетях с применением стека протоколов TCP/IP. При ее построении за основу была взята система Bro. Одним из ее преимуществ является гибкая расширяемость функциональных возможностей за счет написания дополнительных скриптов для обработки сетевых событий. Это позволяет встраивать необходимые сценарии, предназначенные для формирования параметров сессии. Для анализа таких параметров предложены три модуля, которые основаны на различных адаптивных моделях: нейронных сетях, иммунных детекторах и нейронечетких классификаторах. Эксперименты проведены на двух наборах данных: KDD Cup 99 и NSL-KDD. Полученные результаты показали, что в сравнении с существующими подходами к обнаружению, оцененными на данных наборах, предложенная схема комплексирования позволяет достичь компромисса между распознаванием неизвестных типов угроз и ложными срабатываниями. Дальнейшее исследование будет направлено на поиск и применение других гибридных подходов к обнаружению атак, создание экспериментальных наборов данных и проведение экспериментов.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451) и программы фундаментальных исследований ОНИТ РАН (контракт № 1.5).

Литература

1. **Silva L., Santos A., Silva J., Montes A.** A Neural Network Application for Attack Detection in Computer Networks // Proc. of Intern. Joint Conf. on Neural Network. 2004. Vol. 2. P. 1569–1574.
2. **Vollmer T., Manic M.** Computationally Efficient Neural Network Intrusion Detection Security Awareness // 2nd Intern. Symp. on Resilient Control Systems. 2009. P. 25–30.
3. **Lei J. Z., Ghorbani A.** Network Intrusion Detection Using an Improved Competitive Learning Neural Network // Proc. of Second Annual Conf. on Communication Networks and Services Research. 2004. P. 190–197.
4. **Wang G., Hao J., Ma J., Huang L.** A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering // Expert Systems with Applications. 2010. Vol. 37. Iss. 9. P. 6225–6232.
5. **Lei J. Z., Ghorbani A. A.** Improved Competitive Learning Neural Networks for Network Intrusion and Fraud Detection // Neurocomputing. 2012. Vol. 75. Iss. 1. P. 135–145.

6. **Cannady J.** Artificial Neural Networks for Misuse Detection // Proc. of National Information Systems Security Conf. 1998. P. 368–381.
7. **Hofmeyr S. A., Forrest S.** Architecture for an Artificial Immune System // Journal of Evolutionary Computation. 2000. Vol. 8. N 4. P. 443–473.
8. **Hofmeyr S. A.** An Immunological Model of Distributed Detection and its Application to Computer Security: PhD dissertation. — Department of Computer Sciences, University of New Mexico. 1999. — 113 p.
9. **Powers S. T., He J.** A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection // Information Sciences. 2008. Vol. 178. Iss. 15. P. 3024–3042.
10. **Zhou Y. P.** Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection // Asia-Pacific Conf. on Information Processing. 2009. Vol. 1. P. 21–24.
11. **Toosi A. N., Kahani M., Monsefi R.** Network Intrusion Detection Based on Neuro-Fuzzy Classification // Proc. of Intern. Conf. on Computing and Informatics. 2006. P. 1–5.
12. **Orang Z. A.,** et al. Using Adaptive Neuro-Fuzzy Inference System in Alert Management of Intrusion Detection Systems // Intern. Journal of Computer Network and Information Security. 2012. Vol. 4. N 11. P. 32–38.
13. **Zainal A., Maarof M. A., Shamsuddin S. M.** Ensemble Classifiers for Network Intrusion Detection System // Information Assurance and Security. 2009. Vol. 4. P. 217–225.
14. **Vaitsekhovich L.** Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors // XI Intern. PhD Workshop OWD. 2009. P. 219–224.
15. **Komar M., Golovko V., Sachenko A., Bezobrazov S.** Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification // IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). 2013. Vol. 2. P. 665–668.
16. **Golovko V., Komar M., Sachenko A.** Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers // Intern. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). 2010. P. 237.
17. **Govindarajan M., Chandrasekaran R. M.** Intrusion Detection Using an Ensemble of Classification Methods // Proc. of the World Congress on Engineering and Computer Science. 2012. Vol. 1. P. 459–464.
18. **Mukkamala S., Sung A. H., Abraham A.** Intrusion Detection Using Ensemble of Soft Computing Paradigms // Intelligent Systems Design and Applications, Advances in Soft Computing. 2003. Vol. 23. P. 239–248.
19. **Mukkamala S., Sung A. H., Abraham A.** Intrusion Detection Using an Ensemble of Intelligent Paradigms // Journal of Network and Computer Applications. 2005. Vol. 28. Iss. 2. P. 167–182.
20. **Toosi A. N., Kahani M.** A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model Using Neuro-Fuzzy Classifiers // Computer Communications. 2007. Vol. 30. Iss. 10. P. 2201–2212.
21. **Riedmiller M., Braun H.** A Direct Adaptive Method for Faster Backpropagation Learning: The RPROP Algorithm // IEEE Intern. Conf. on Neural Networks. 1993. P. 586–591.
22. **Bro 2.3.2** documentation. https://www.bro.org/documentation/index.html (дата обращения: 10.02.2015).
23. **Syarif I., Zaluska E., Prugel-Bennett A., Wills G.** Application of Bagging, Boosting and Stacking to Intrusion Detection // Machine Learning and Data Mining in Pattern Recognition. 2012. Vol. 7376. P. 593-602.
24. **Merz C. J.** Combining Classifiers Using Correspondence Analysis // Advances in Neural Information Processing. 1997. P. 591–597.
25. **Prodromidis A., Chan P., Stolfo S.** Meta-Learning in Distributed Data Mining Systems: Issues and Approaches // Advances in Distributed and Parallel Knowledge Discovery. 2000. P. 81–113.
26. **Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.** Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. 2012. Вып. 1(20). С. 27–56.
27. **Федорченко А. В., Чечулин А. А., Котенко И. В.** Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей // Информационно-управляющие системы. 2014. № 5. С. 72–79.

UDC 004.056
doi:10.15217/issn1684-8853.2015.4.69

Network Attack Detection Based on Combination of Neural, Immune and Neuro-fuzzy Classifiers

Branitskiy A. A.[a], Junior Researcher, branitskiy@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Head of Laboratory of Computer Security Problems, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: Imperfection of existing methods of intrusion detection and changing nature of malicious actions of the attackers lead computer systems to a compromised state. Therefore, it is important to identify new types of attacks and respond timely to them.

Purpose: The development of a hybrid scheme of detection and classification of network attacks based on a combination of adaptive classifiers. **Results:** The generalized scheme of combining the classifiers to detect network attacks is offered. On its basis the software tool is developed which enables to analyze network traffic for anomalous network activity. To reduce the number of input features it is proposed to use the principal component analysis. The key features of the technique is a multi-level analysis of network traffic and using different adaptive modules while detecting the attacks. Computational experiments are performed on two public datasets using different means of combining classifiers. **Practical relevance:** Developed modules can be used for processing the data received from the security information and event management system.

Keywords — Intrusion Detection, Network Attacks, Neural Networks, Immune Detectors, Neuro-Fuzzy Classifiers, Principal Component Analysis.

References

1. Silva L., Santos A., Silva J., Montes A. A Neural Network Application for Attack Detection in Computer Networks. *Proc. of Intern. Joint Conf. on Neural Network*, 2004, vol. 2, pp. 1569–1574.
2. Vollmer T., Manic M. Computationally Efficient Neural Network Intrusion Detection Security Awareness. *2nd Intern. Symp. on Resilient Control Systems*, 2009, pp. 25–30.
3. Lei J. Z., Ghorbani A. Network Intrusion Detection Using an Improved Competitive Learning Neural Network. *Proc. of Second Annual Conf. on Communication Networks and Services Research*, 2004, pp. 190–197.
4. Wang G., Hao J., Ma J., Huang L. A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering. *Expert Systems with Applications*, 2010, vol. 37, iss. 9, pp. 6225–6232.
5. Lei J. Z., Ghorbani A. A. Improved Competitive Learning Neural Networks for Network Intrusion and Fraud Detection. *Neurocomputing*, 2012, vol. 75, iss. 1, pp. 135–145.
6. Cannady J. Artificial Neural Networks for Misuse Detection. *Proc. of National Information Systems Security Conf.*, 1998, pp. 368–381.
7. Hofmeyr S. A., Forrest S. Architecture for an Artificial Immune System. *Journal of Evolutionary Computation*, 2000, vol. 8, no. 4, pp. 443–473.
8. Hofmeyr S. A. *An Immunological Model of Distributed Detection and its Application to Computer Security*. PhD dissertation. Department of Computer Sciences, University of New Mexico, 1999. 113 p.
9. Powers S. T., He J. A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection. *Information Sciences*, 2008, vol. 178, iss. 15, pp. 3024–3042.
10. Zhou Y. P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection. *Asia-Pacific Conf. on Information Processing*, 2009, vol. 1, pp. 21–24.
11. Toosi A. N., Kahani M., Monsefi R. Network Intrusion Detection Based on Neuro-Fuzzy Classification. *Proc. of Intern. Conf. on Computing and Informatics*, 2006, pp. 1–5.
12. Orang Z. A., Moradpour E., Navin A. H., Ahrabim A. A. A., Mirnia M. K. Using Adaptive Neuro-Fuzzy Inference System in Alert Management of Intrusion Detection Systems. *Intern. Journal of Computer Network and Information Security*, 2012, vol. 4, no. 11, pp. 32–38.
13. Zainal A., Maarof M. A., Shamsuddin S. M. Ensemble Classifiers for Network Intrusion Detection System. *Information Assurance and Security*, 2009, vol. 4, pp. 217–225.
14. Vaitsekhovich L. Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors. *XI Intern. PhD Workshop OWD*, 2009, pp. 219–224.
15. Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification. *IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, 2013, vol. 2, pp. 665–668.
16. Golovko V., Komar M., Sachenko A. Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers. *Intern. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2010, p. 237.
17. Govindarajan M., Chandrasekaran R. M. Intrusion Detection Using an Ensemble of Classification Methods. *Proc. of the World Congress on Engineering and Computer Science*, 2012, vol. 1, pp. 459–464.
18. Mukkamala S., Sung A. H., Abraham A. Intrusion Detection Using Ensemble of Soft Computing Paradigms. *Intelligent Systems Design and Applications, Advances in Soft Computing*, 2003, vol. 23, pp. 239–248.
19. Mukkamala S., Sung A. H., Abraham A. Intrusion Detection Using an Ensemble of Intelligent Paradigms. *Journal of Network and Computer Applications*, 2005, vol. 28, iss. 2, pp. 167–182.
20. Toosi A. N., Kahani M. A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model Using Neuro-Fuzzy Classifiers. *Computer Communications*, 2007, vol. 30, iss. 10, pp. 2201–2212.
21. Riedmiller M., Braun H. A Direct Adaptive Method for Faster Backpropagation Learning: The RPROP Algorithm. *IEEE Intern. Conf. on Neural Networks*, 1993, pp. 586–591.
22. *Bro 2.3.2 documentation*. Available at: https://www.bro.org/documentation/index.html (accessed 10 February 2015).
23. Syarif I., Zaluska E., Prugel-Bennett A., Wills G. Application of Bagging, Boosting and Stacking to Intrusion Detection. *Machine Learning and Data Mining in Pattern Recognition*, 2012, vol. 7376, pp. 593–602.
24. Merz C. J. Combining Classifiers Using Correspondence Analysis. *Advances in Neural Information Processing*, 1997, pp. 591–597.
25. Prodromidis A., Chan P., Stolfo S. Meta-Learning in Distributed Data Mining Systems: Issues and Approaches. *Advances in Distributed and Parallel Knowledge Discovery*, 2000, pp. 81–113.
26. Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A. Application of Security Information and Event Management Technology for Information Security in Critical Infrastructures. *Trudy SPIIRAN*, 2012, iss. 1(20), pp. 27–56 (In Russian).
27. Fedorchenko A. V., Chechulin A. A., Kotenko I. V. Open Vulnerability Bases and their Application in Security Analysis Systems of Computer Networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5, pp. 72–79 (In Russian).