УДК 004.056.53; 004.89

НЕЙРОСЕТЕВОЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

М.П. Комар[1], И.О. Палий[1], Р.П. Шевчук[1], Т.Б. Федысив[2]

[1] Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: mko@tneu.edu.ua
[2] Государственное высшее учебное заведение «Дрогобычский механико-технологический колледж»,
ул. Раневицька, 12, 82100, Дрогобыч, Украина; e-mail: f_taras2006@ukr.net

В работе произведен выбор нейронной сети для обнаружения сетевых атак. Предложен способ формирования обучающей выборки для обучения нейросетевого детектора. Представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика. Представлены результаты экспериментальных исследований.

Ключевые слова: нейронная сеть, сетевая атака, нейросетевой детектор, метод главных компонент, сетевой трафик

Введение

Произведенный анализ методов и средств защиты компьютерных систем от сетевых атак показывает, что нейросетевые методы продолжают стремительно развиваться, причем основная тенденция – применение комбинаций нейронных сетей с другими методами.

Благодаря своим особенностям, таким как высокая степень параллелизма обработки информации, способность к обобщению, адаптация к изменениям окружающей среды, распознавание зашумленных образов, низкий уровень ресурсоемкости и т.д., нейронные сети позволяют достичь хороших результатов в решении таких сложных инженерных задач как распознавание образов, классификация, прогнозирование, системы контроля и т.д. В связи со способностью искусственных нейронных сетей в процессе обучения выявлять сложные зависимости между входными и выходными данными, которые отсутствовали в обучающей выборке, и, способностью корректно классифицировать зашумленные образы, они являются привлекательным инструментом для решения сложных разнообразных задач защиты компьютерной информации.

Все это послужило базой для выбора искусственных нейронных сетей в качестве основного инструмента обнаружения компьютерных атак.

В работе исследуются разнообразные архитектуры нейронных сетей с целью выбора нейронной сети для обнаружения сетевых атак, предложен способ формирования обучающей выборки для обучения нейросетевого детектора, представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика и представлены результаты экспериментальных исследований.

Выбор архитектуры нейронной сети для обнаружения компьютерных атак

Существует большое количество нейронных сетей, применяемых для решения тех

или иных сложных инженерных задач. Так многослойные персептроны (multilayer perceptron – MLP) [1] характеризуется прямым распространением входного сигнала от слоя к слою и состоят из множества входных нейронных элементов, одного или нескольких скрытых слоев нейронных элементов, и выходного слоя. Одним из главных преимуществ таких сетей является возможность решать алгоритмически неразрешимые задачи или задачи, для которых алгоритмическое решение неизвестно, но для которых возможно составить репрезентативный набор примеров с известными решениями. MLP при обучении, за счёт своего внутреннего строения, выявляет закономерности в связи входных и выходных образов и тем самым обобщает полученный на обучающей выборке опыт.

Рекуррентные нейронные сети [1] имеют обратные связи между слоями нейронов, т.е. выходы нейронных элементов последующих слоев связаны с нейронами предшествующих слоев. Таким образом, происходит учет результатов преобразование нейронной сетью информации на предыдущем этапе для обработки входного вектора на следующем этапе функционирования сети. Рекуррентные сети могут использоваться для решения задач прогнозирования и управления.

Рециркуляционные нейронные сети (recirculation neural networks - RNN) [1] предназначены для сжатия (прямое преобразование) и восстановления (обратное преобразование) исходной информации и характеризуются как прямым так и обратным преобразованием информации.

Нейронные сети с радиально-базисной функцией активации (radial basis function networks - RBF) [1] применяются для решения задач прогнозирования, аппроксимации функций, распознавания образов и т.д.

Нейронные сети Кохонена позволяют в результате обучения осуществлять топологически непрерывное отображение F-входного n-мерного пространства в выходное m-мерное пространство. Структура такой нейронной сети представляет собой сеть с прямым распространением сигнала. В качестве метода обучения используется конкурентное обучение. По мере поступления входных образов на такую сеть посредством обучения происходит разбиение n-мерного входного пространства на различные области решений, каждой из которых соответствует отдельный нейрон.

Нейронные сети для векторного квантования (LVQ) используются для сжатия данных и основаны на идее сопоставления входного вектора с эталоном. В процессе поступления эталонных векторов на сеть она обучается так, что образуются кластеры различных эталонов, каждому из которых соответствует свой нейрон. При поступлении на вход такой нейронной сети неизвестного образа, он идентифицируется в соответствии с мерой близости к эталонным векторам и кодируется на выходе сети номером нейрона.

К системе обнаружения вторжений предъявляется ряд жестких требований, одним из которых является функционирование в режиме реального времени. В результате, необходимо минимизировать временные затраты, связанные с обучением нейронной сети. В результате, необходимо выбрать такую архитектуру, которая бы характеризовалась минимальным временем обучения, а, следовательно, и минимальным размером обучающей выборки. Рассмотрим характеристики MLP [1,2]. Многослойные персептроны обучаются при мощи алгоритма обратного распространения ошибки (back-propagation algorithm) [1,2] и успешно применяются решения многих сложных задач классификации, распознавания и др. В [2] сказано, что на способность нейронной сети к корректному обобщению влияют размер обучающей выборки и архитектура нейронной сети. В нашем случае количество входных нейронов должно равняться количеству атрибутов сетевого трафика, т.е. $n = 41$. Количество скрытых нейронов согласно проведенным экспериментам должно равняться $m = 10$. Количество выходных нейронов равняется $k = 2$, т.е. каждый из выходных нейронов отображает тот или иной класс входного образа.

Для корректного обучения нейронной сети достаточно, чтобы размер обучающей выборки L удовлетворял следующему соотношению [2]:

$$L = O(W / \varepsilon), \tag{1}$$

где W – общее количество настраиваемых параметров (весовых коэффициентов и пороговых значений); ε - допустимая точность ошибки классификации; $O(\ldots)$ – порядок величины, т.е., например, для ошибки в 5% количество примеров обучения должно в 5 раз превосходить количество свободных параметров сети W.

Общее количество настраиваемых параметров вычисляется согласно следующему выражению:

$$W = m(n+3)+2. \tag{2}$$

В результате, в случае применения MLP в качестве детектора для обнаружения сетевых атак обучающая выборка для обучения нейронной сети с допустимой ошибкой классификации $\varepsilon = 0{,}1$ должна состоять, согласно выражениям (1) и (2) из 4420 образов.

Проведем аналогичный анализ для RBF сетей [1,2]. Сети на основе радиальных базисных функций также являются многослойными нейронными сетями. Первый слой таких сетей является входным слоем и обеспечивает связь сети с внешней средой. Второй слой – скрытый слой, выполняет нелинейное преобразование входное пространство образов в скрытое пространство, зачастую имеющее существенно более высокую размерность, чем входное. Третий слой – выходной, он состоит из линейных нейронов. В [2] сказано, что формулы (1) и (2) в общем случае применимы и для сетей RBF, т.е. для корректного обучения детектора на основе RBF сети нам также необходимо, чтобы размер обучающей выборки был равным 4420 образов. Более того, известно, что чем выше число скрытых нейронов сети RBF тем выше качество классификации в определенных задачах. Так, например, в [2] показано, что при увеличении количества центров с 20 до 100, качество классификации увеличивается примерно на 4,5%. Таким образом, для повышения качества распознавания сетевых атак на основе RBF сети необходима обучающая выборка большего размера.

Теперь рассмотрим сеть встречного распространения [1,2] с идентичным количеством нейронов в каждом из слоев. В скрытом слое такой сети будем использовать нейронные элементы Кохонена [1-3]. Для обучения такой сети достаточно, чтобы размер обучающей выборки был равным согласно следующему выражению [2]:

$$L \geq 2m. \tag{3}$$

Таким образом, для обучения сети встречного распространения с нейронами Кохонена в скрытом слое необходимо иметь обучающую выборку с размерностью равной минимум 82 образам. В результате, основываясь на выдвинутых ранее требованиях к системе обнаружения вторжений, выберем данную нейронную сеть в качестве основы нейросетевого детектора.

Формирование обучающей выборки

Структура нейросетевого детектора для обнаружения сетевых атак и метод обучения многослойной нейронной сети с входным слоем, одним скрытым слоем, состоящим из нейронов Кохонена [1,3], и выходным слоем представлены в [4-6].

В качестве входных данных для нейросетевых детекторов использовались дан-

ные, взятые из базы данных KDD Cup1999 Data [7].

Для обучения предложенного нейросетевого детектора используется обучающая выборка, состоящая из 80% соединений одного из типов атак и 20% нормального соединения, т.е. соотношение атак к нормальным соединениям равняется четыре к одному.

Такое соотношение было получено экспериментальным путем и показало наилучшие результаты классификации сетевого трафика (результаты экспериментов представлены в таблице 1).

Таблица 1.

Результаты обнаружения DoS-атак

Тип атаки	5/1	4/1	3/1	2/1	1/1
DoS	95,7%	98,0%	97,5%	96,4%	96,0%
Probe	59,2%	65,1%	63,9%	62,1%	61,5%
R2L	32,4%	36,9%	34,8%	33,9%	33,0%
U2R	16,8%	20,8%	19,0%	18,7%	17,1%

Было проведено 5 экспериментов. В каждом эксперименте генерировались 20 нейросетевых детекторов. В первом эксперименте для обучения нейронной сети использовалась такая обучающая выборка, в которой соотношение нормальных сетевых соединений к атакам составляло пять к одному. Во втором эксперименте соотношение классов сетевых соединений равнялось четыре к одному, в третьем – три к одному, в четвертом – два к одному. В последнем эксперименте обучающая выборка состояла из 50% нормального трафика и 50% сетевых атак. Сгенерированные детекторы обучались и классифицировали неизвестные образы. Результаты классификации представлены в таблице 1. Как видно из таблицы 1, наилучший результат показали те детекторы, для обучения которых использовалась выборка, состоящая из 80% сетевых атак и 20% нормальных сетевых соединений.

Исходя из того, что классы сетевого трафика распределены в обучающей выборке в соотношении 80% сетевых атак и 20% нормальных соединений, то это налагает определенные требования на распределение нейронов Кохонена в скрытом слое нейросетевого детектора. Для корректного функционирования выбранной нейронной сети необходимо, чтобы соотношение между количеством нейронов в слое Кохонена, характеризующие различные классы, должно быть кратным соотношению четыре к одному.

Таким образом, соотношение нейронов в скрытом слое должно быть равным

$$f/1 = 4/1, \qquad (4)$$

где f – первые нейроны слоя Кохонена, активность которых характеризует сетевую атаку; 1 – последние нейроны слоя Кохонена, активность которых характеризует нормальное сетевое соединение.

В результате, если количество нейронов Кохонена в скрытом слое равняется десяти, то количество нейронов, отвечающих за сетевую атаку, будет равным $f = 8$, а количество нейронов, отвечающих за нормальное соединение, будет равным $1 = 2$.

Применение метода главных компонент

Для сокращения размера данных при обучении и анализе сетевого трафика предлагается использовать метод главных компонент [8].

В общем виде метод главных компонент можно представить в виде следующей формулы:

$$X = TP^T + E, \tag{5}$$

где X – матрица данных, каждая строка которой является вектором предобработанных данных. Матрицу данных можно представить в следующем виде: $X = \{x_1,...x_m\}^T$, где m – число векторов данных, n – размерность пространства данных; P – матрица нагрузок, в которой каждый столбец отображает вектор главных компонент. Матрицу нагрузок можно представить в следующем виде: $P = \{a_1,...a_k\}$, где k – количество векторов главных компонент, выбранных для проецирования; T – матрица счетов, в которой каждая строка представляет собой проекцию вектора данных на k главных компонент. Матрицу счетов можно представить в виде $T = \lfloor t_{ij} \rfloor$, где $t_{ij} = (x_i, a_j)$; E – матрица ошибок, вычисляемая по формуле $E = X - TP^T$.

Анализируя распределение количества информации, содержащейся в каждой последующей главной компоненте, можно определить число компонент, которые целесообразно использовать для дальнейшего анализа.

На рис. 1 представлена зависимость количества информации от числа главных компонент.

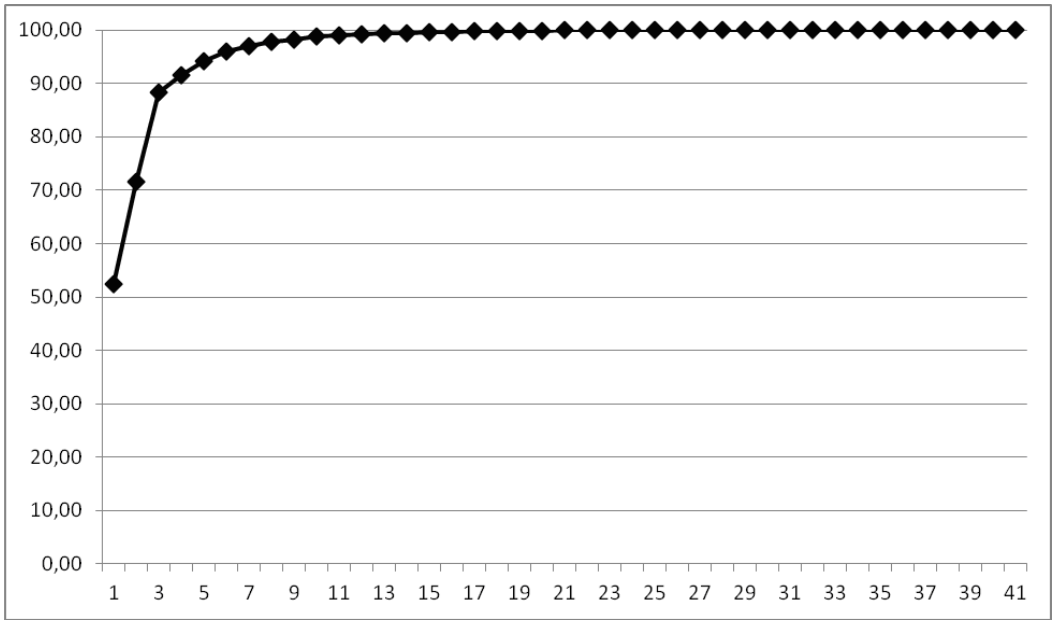

Рис. 1. Зависимость количества информации от числа главных компонент

Как видно из рис. 1 первых главных компонент содержат 99% информации о сетевом трафике. В остальных 30 компонентах содержится только 1% информации, и из соображения целесообразности их можно исключить из анализа.

Использование метода главных компонент выявило тот факт, что для успешного анализа сетевого трафика достаточно использовать 12 первых главных компонент, в которых содержится 99% информации о сетевом соединении, а не 41 параметр. Это позволит существенно ускорить как процесс обучения нейросетевого детектора, так и процесс анализа сетевого трафика. Для этого, к выделенным из сетевого трафика применяем сначала метод главных компонент, а затем, подаем полученные данные на вход нейронной сети.

Схематически данный процесс изображен на рис. 2.

Рис. 2. Взаимодействие связки PCA и нейросетевой детектор

При таком подходе, количество n входных нейронов используемой нейронной сети в качестве детектора равняется 12. Подаваемая информация – двенадцать первых главных компонент, подаются на скрытый слой детектора, где и происходит его определение к классу сетевой атаки или к классу легитимного соединения.

Сравнительный анализ результатов обнаружения сетевых атак с применением метода главных компонент и без PCA представлены в таблицах 2–5.

Таблица 2.

Сравнительный анализ результатов обнаружения DoS-атак

	Back, %	Land, %	Neptune, %	Pod, %	Smurf, %	Teardrop, %	Среднее по атакам, %
PCA	99,5	100,0	100,0	98,1	100,0	100,0	99,6
без PCA	99,5	90,5	100,0	98,1	100,0	100,0	98,0
Улучшение	0	9,5	0,0	0,0	0,0	0,0	1,6

Таблица 3.

Сравнительный анализ результатов обнаружения Probe-атак

	Ipsweep, %	Nmap, %	Portsweep, %	Satan, %	Среднее по атакам, %
PCA	65,2	100,0	99,9	99,3	91,1
без PCA	7,1	54,5	99,6	99,3	65,1
Улучшение	58,1	45,5	0,3	0,0	26%

Таблица 4.

Сравнительный анализ результатов обнаружения R2L-атак

	Ftp_write, %	Guess_passwd, %	Imap, %	Multihop, %	Phf, %	Spy, %	Warezclient, %	Warezmaster, %	Среднее по атакам, %
PCA	100,0	94,3	83,3	57,1	100,0	100,0	65,0	90,0	86,2
без PCA	25,0	0,0	50,0	28,6	100,0	0,0	32,0	80,0	36,9
Улучшение	75,0	94,3	33,3	28,5	0,0	100,0	33,0	10,0	49,3

Таблица 5.

Сравнительный анализ результатов обнаружения U2R-атак

	Buffer_overflow, %	Loadmodule, %	Perl, %	Rootkit, %	Среднее по атакам, %
PCA	83,3	100,0	33,3	30,0	61,7
без PCA	63,3	0,0	0,0	20,0	20,8
Улучшение	20,0	100,0	33,3	10,0	40,9

Как видно из полученных результатов, качество обнаружения удалось значительно увеличить благодаря применению метода главных компонент к параметрам сетевого трафика. Так прирост в качестве обнаружения в среднем для DoS-атак составил 1,6 %, для Probe-атак составил 26,0%, для R2L-атак составил 49,3%, для U2R-атак составил 40,9%.

Следует отметить, что процент возникновения ложного обнаружения составляет менее 1,7%.

Также, за счет того, что для анализа сетевого трафика теперь используются не все 41 параметр, а 12 главных компонент, удалось значительно повысить быстродействие системы в целом, что является важным критерием для систем защиты информации.

Заключение

В данной работе в качестве нейросетевого детектора для обнаружения сетевых атак выбрана многослойная нейронная сеть с входным слоем, одним скрытым слоем, состоящим из нейронов Кохонена, и выходным слоем. Для обучении нейросетевого детектора используется обучающая выборка, состоящая из 80% соединений, относящихся к сетевым атакам, и 20% соединений, относящихся к нормальным соединениям.

Также, представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика с целью выявления компьютерных атак. Применение PCA позволило повысить качество обнаружения сетевых атак на компьютерные системы, а также повысить быстродействие системы за счет сокращения анализируемых данных. Однако, некоторые типы атак, такие как ipsweep, multihop, warezclient, perl и rootkit, недостаточно хорошо обнаруживаются. Для преодоления этого недостатка предлагается применить метод искусственных иммунных систем.

Список литературы

1. Головко В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение: учеб. пособие / В.А. Головко. – М., 2001 – 256 с.
2. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.

3. Kohonen T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – N43. – P. 59–69.
4. Комар М.П. Система анализа сетевого трафика для обнаружения компьютерных атак / М.П. Комар // Вестник Брестского государственного технического университета: (Серия: физика, математика и информатика). – 2010. – №5. – С. 14–16.
5. Комар М. Методы искусственных нейронных сетей для обнаружения сетевых вторжений / М. Комар // Сборник тезисов седьмой международной научно-технической конференции "Интернет - Образование - Наука " (ИОН-2010) – Винница: Винницкий национальный технический университет, 2010. – С. 410–413.
6. Комар М.П. Интеллектуализированная информационная технология обнаружения компьютерных атак / М.П. Комар, Д.И. Боднар, А.А. Саченко // Измерительная и вычислительная техника в технологических процессах. – 2010. – № 2. – С. 133–137.
7. KDD Cup 1999 Data [Электронный ресурс]. – Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
8. Jolliffe, I. Principal component analysis / I.T. Jolliffe. – Springer, 2010. – 516 p.

М.П. Комар, І.О. Палій, Р.П. Шевчук, Т.Б. Федисів

НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК НА КОМП'ЮТЕРНІ СИСТЕМИ

Зроблено вибір нейронної мережі для виявлення мережевих атак. Запропоновано спосіб формування навчальної вибірки для навчання нейромережевого детектора. Представлено застосування методу головних компонент для скорочення розміру даних для аналізу мережевого трафіку. Представлені результати експериментальних досліджень.

Ключові слова: нейронна мережа, комп'ютерна атака, нейромережевий детектор, метод головних компонент, мережевий трафік

M. Komar, I. Paliy, R. Shevchuk, T. Fedysiv

NEURAL NETWORK APPROACH FOR DETECTION OF NETWORK ATTACKS ON COMPUTER SYSTEMS

We made the choice of a neural network to detect network attacks. The method that forms the training set for neural network detector training. Is proposed the use of principal component analysis to reduce the size of data for analyzation of network traffic is presented. The results of experimental studies are presented.

Keywords: neural network, network attack, neural network detector, the method of principal components analysis, the network traffic